

Privacy and Efficacy of  
Electronic Health Records (EHRs):  
A Triangulation Study in Ontario, Canada

A thesis submitted to the University of Manchester  
for the degree of  
Doctor of Business Administration  
in the Faculty of Humanities

2018

Roy K. Ng

Alliance Manchester Business School

## Table of Contents

<b>Table of Contents .....</b>	<b>2</b>
<b>List of Figures.....</b>	<b>7</b>
<b>List of Tables .....</b>	<b>9</b>
<b>Abstract.....</b>	<b>11</b>
<b>Chapter 1 Introduction.....</b>	<b>15</b>
1.1 Introduction .....	15
1.2 Background .....	15
1.3 The Definition and the Concepts of Privacy .....	17
1.3.1 <i>The Concepts of Privacy and its Extension to Electronic Health Records (EHRs).....</i>	<i>18</i>
1.4 The Many Names of EHR and Definition Used in This Research.....	20
1.5 Three Different Stakeholders Using Different Domains in EHR.....	23
1.6 Pan-Canadian Implementation of EHR .....	25
1.7 Patient Concerns About Their Privacy in EHR.....	27
1.8 Will This Happen in Canada? .....	28
1.9 The Implication of Privacy and Security Issues with EHR.....	29
1.10 Protection of Personal Health Information in Ontario .....	31
1.11 Research Question and Importance of This Research.....	33
1.12 Thesis Structure .....	35
1.13 Chapter Summary .....	36
<b>Chapter 2 Literature Review .....</b>	<b>37</b>
2.1 Introduction .....	37
2.2 Conducting the Literature Review .....	37
2.3 Worldwide Approach and Implementation of EHR.....	38
2.4 Costs and Benefits of EHR.....	44
2.5 What Are the Issues in EHR Especially in Privacy and Security Protection?.....	48
2.6 The literature on Assessment Model of Privacy and EHR.....	54
2.7 Gaps in the Literature .....	55
2.8 Research Questions .....	57
2.8.1 <i>Research Sub-questions.....</i>	<i>58</i>
2.9 Concepts of Countermeasures .....	58
2.10 Validity and Relevancy of This Literature Review .....	59
2.11 Chapter Summary .....	62
<b>Chapter 3 Research Methodology and Design .....</b>	<b>63</b>
3.1 Introduction .....	63
3.2 Propositional Knowledge in This Research .....	63
3.3 Philosophical Position of this Research .....	66
3.4 Critical Realism .....	67
3.5 Research Methods .....	69

3.6	Research Models .....	71
3.6.1	<i>Using the 3Ps models for Three Different Stakeholders Group.....</i>	71
3.6.2	<i>Concerns For Information Privacy (CFIP) Framework.....</i>	73
3.7	Theoretical Framework and Hypothesis.....	74
3.7.1	<i>Patients.....</i>	75
3.7.2	<i>Service Providers .....</i>	77
3.7.3	<i>Payers.....</i>	78
3.8	Research Design .....	78
3.8.1	<i>Patients.....</i>	79
3.8.2	<i>Providers .....</i>	84
3.8.3	<i>Payers.....</i>	86
3.9	Synthesizing and Validating the Findings Using Triangulation Design	89
3.10	The justification for Human Involvement .....	92
3.11	Study Location .....	92
3.12	Chapter Summary .....	93
<b>Chapter 4 Results of Patients' Survey .....</b>		<b>94</b>
4.1	Introduction .....	94
4.2	Survey to Study Patient Attitudes .....	96
4.2.1	<i>Sampling Groups and Triangulation of the Survey.....</i>	96
4.2.2	<i>Structure of Questionnaires.....</i>	98
4.2.3	<i>Data Integrity and Cleaning.....</i>	101
4.2.4	<i>Survey Instrument.....</i>	101
4.3	Validity and Reliability of the Survey Instrument .....	102
4.3.1	<i>Content Validity.....</i>	103
4.3.2	<i>Criterion Validity .....</i>	105
4.3.2.1	<i>Concurrent Validity .....</i>	105
4.3.3	<i>Construct Validity.....</i>	106
4.3.4	<i>CFIP Model: A Validated Instrument for Research on Information Privacy.....</i>	107
4.4	Descriptive Statistics of the Survey.....	108
4.5	Overall Result of the Concern For Information Privacy (CFIP) Dimensions .....	112
4.5.1	<i>DIMENSION 1: Privacy Concerns on Unauthorized Secondary Use of Information.....</i>	115
(A)	No Other Purpose (NOP) .....	116
(B)	No Other Unrelated Reasons (NOU).....	118
(C)	Never Sell Information (NSI).....	119
(D)	No Unauthorized Sharing (NUS) .....	121
4.5.2	<i>DIMENSION 2: Privacy Concerns on Improper Access .....</i>	122
(A)	Efforts to Prevent Unauthorized Access (EUA).....	123
(B)	Databases Protected from Unauthorized access (DPU) .....	125
(C)	Protection of Unauthorized Access (PUA) .....	127
4.5.3	<i>DIMENSION 3: Privacy Concerns of Information Errors .....</i>	128
(A)	Accuracy Regardless of Cost (ARC).....	129
(B)	Necessary Steps for Accuracy (NSA) .....	131
(C)	Correct Errors Timely (CET) .....	132
(D)	Verify Accuracy of Information (VAI) .....	134

4.5.4	<i>DIMENSION 4: Privacy Concerns on Too Much Collection</i> .....	136
(A)	Bothers Me When Asked for Personal Health Information (BGI).....	136
(B)	It Bothers Me to Give So Much Information (BMI) .....	138
(C)	Too Much Information is Collected (MIC) .....	140
(D)	Think Twice Before Disclosure (TTD) .....	142
4.6	Age Modeled via Career Stage.....	144
4.6.1	<i>Early Career Cluster: (18 – 35 years. old)</i> .....	146
4.6.2	<i>Mid-Career Stage Cluster: (36 – 55 yr. old)</i> .....	148
4.6.3	<i>Late-Career Stage Cluster: (ages 56+)</i> .....	148
4.7	Results of Findings in Career Stage Cluster.....	149
4.7.1	<i>Concerns of Error</i> .....	149
4.7.2	<i>Concerns of Improper Access</i> .....	151
4.7.3	<i>Concerns about Secondary Use</i> .....	152
4.7.4	<i>Concerns of Collection</i> .....	154
4.8	Response by Gender .....	155
4.9	The result of Scenario Questions.....	158
4.9.1	<i>Purpose of Scenario Questions</i> .....	158
4.9.2	<i>Share Information Without Consent (SSWC)</i> .....	158
4.9.3	<i>Disclosure May Result In Social Rejection (SDSR)</i> .....	160
4.9.4	<i>Disclose may result in a financial loss (SDFL)</i> .....	161
4.9.5	<i>Disclosure with countermeasure (SDWC)</i> .....	163
4.9.6	<i>Disclosure when in an emergency (SDWE)</i> .....	165
4.9.7	<i>Control data privacy (SCDP)</i> .....	166
4.10	Overall Attitude Towards Service Provider .....	168
4.10.1	<i>Provider Can Keep Data Secure And Private (DSP)</i> .....	168
4.10.2	<i>Willing to Give Information if Sickesses Worsens (WIW)</i> .....	170
4.11	Emerging Themes.....	171
4.12	Preliminary Findings on patient's response towards the research sub- questions .....	172
4.13	Other Observed Preliminary Findings.....	173
4.14	Chapter Summary .....	175
<b>Chapter 5 Results of Focus Group Meetings with Providers</b> .....		<b>176</b>
5.1	Introduction .....	176
5.2	Using Focus Group Discussion with Service Provider .....	176
5.3	Methodology in conducting the focus group discussion .....	178
5.3.1	<i>Enrollment</i> .....	178
5.3.2	<i>Focus Group Settings and Data Processing</i> .....	179
5.3.3	<i>Professional requirements to protect patient's private information</i> ..	180
5.4	Results of Focus Group One: Nurses and Pharmacists .....	181
5.4.1	<i>EHR benefits and risks</i> .....	182
5.4.2	<i>The Need and Protection of Patient's Private Information</i> .....	184
5.4.3	<i>Patient Countermeasures to Service Provider's Need of Private Information</i> .....	193
5.4.4	<i>Provider's Concern of own privacy</i> .....	195
5.4.5	<i>Provider's Countermeasure of Concerns</i> .....	197
5.4.6	<i>Opinion on the Design EHR Related to Provider's Practice</i> .....	197
5.5	The Result of Focus Group Two: Doctors Group .....	200

5.5.1	<i>Benefits and Trade-Off of EHR</i> .....	201
5.5.2	<i>The Need and Protection of Patient Private Information</i> .....	205
5.5.3	<i>Patient Countermeasures to Service Provider</i> .....	208
5.5.4	<i>Providers' Concern of Their Privacy</i> .....	210
5.5.5	<i>Providers' Countermeasure of Concerns</i> .....	212
5.5.6	<i>Efficiency and Design of EHR</i> .....	214
5.5.7	<i>Security protection and Cybercrime</i> .....	214
5.5.8	<i>Computers and doctor-patient interaction</i> .....	215
5.5.9	<i>EHR implementation – how to make it successful?</i> .....	215
5.6	Observations and Emerging Themes from Group Two (doctors) .....	218
5.7	Other Observed Preliminary Findings .....	219
5.8	Preliminary Findings on providers' response towards the research questions .....	220
5.9	Chapter Summary .....	222
<b>Chapter 6 Results of Key Information Interviews with Payers</b> .....		<b>223</b>
6.1	Introduction .....	223
6.1.1	<i>Three Groups of Informants</i> .....	224
6.2	Functions of Key Informant Interviews .....	225
6.3	Methodology in Conducting the Key Informant Interview .....	227
6.4	Results of Key Informant Interviews on pre-questionnaire .....	229
6.4.1	<i>Results of EHR Benefit Statements from the Government Group</i> .....	229
6.4.2	<i>Result Of the EHR Benefit Statements from the Medical Professional Association Group</i> .....	230
6.4.3	<i>Result of the EHR Benefit Statements from the Legal Group</i> .....	231
6.5	Results of Semi-Structured Questions from All Three Groups .....	233
6.5.1	<i>Baseline: Additional Benefits and Barrier to EHR</i> .....	235
6.5.3	<i>Efficacy: Gaps in EHR Design and Implementation</i> .....	242
6.5.4	<i>Probe for Patient Concern</i> .....	245
6.5.5	<i>Overall Project Impact</i> .....	248
6.6	Preliminary Findings on Payers' Response Towards the Research Questions .....	249
6.6.1	<i>Other Observed Preliminary Findings</i> .....	250
6.7	Scope and Limitations of the Evaluation .....	251
6.8	Chapter Summary .....	252
<b>Chapter 7 Research Findings</b> .....		<b>253</b>
7.1	Introduction .....	253
7.2	Quantitative Framework for Patients: Ranking of Privacy Concerns ..	254
7.2.1	<i>Highest Privacy Concern is the Unauthorized Secondary Use</i> .....	256
7.2.2	<i>Second Privacy Concern: Improper Access</i> .....	257
7.2.3	<i>Third Privacy Concern: Error of information</i> .....	258
7.2.4	<i>Fourth Privacy Concern: Too much collection</i> .....	259
7.3	New Intervening Variable Emerged in Patient Qualitative Scenario Survey .....	261
7.4	Providers' Framework: Ability to Provide Quality Care in EHR .....	262
7.5	Payers' Framework: Realization of Benefits .....	263
7.6	Critical realist Interpretation .....	264

7.7	Gender and Age Group.....	265
7.8	Type 3, 2 and 1 Findings after [PF] Triangulation.....	266
7.8.1	<i>Type 3 Findings</i> .....	271
7.8.2	<i>Type 2 findings</i> .....	274
7.8.3	<i>Type 1 findings</i> .....	280
7.9	Five Themes Established from Findings .....	281
7.9.1	<i>Privacy</i> .....	281
7.9.2	<i>Countermeasures</i> .....	285
7.9.3	<i>Efficacy</i> .....	288
7.9.4	<i>Benefits</i> .....	293
7.9.5	<i>Communications and Training</i> .....	294
7.6	Summary .....	296
<b>Chapter 8 Research Questions and Conclusion .....</b>		<b>297</b>
8.1	Introduction .....	297
8.2	Revisit the Research Problem.....	297
8.3	Research Objectives and Findings for Research Sub-Questions.....	298
8.4	Overall Findings from the Research Sub-Questions .....	302
8.5	Findings for the Primary Research Question .....	304
8.6	The Contribution of this Study .....	306
8.7	Limitations of This Research .....	307
8.8	Future Research and High-Level guidelines .....	308
8.9	Conclusion.....	309
8.10	Reflection .....	309
8.10.1	<i>Lesson Learned</i> .....	312
8.10.2	Final Words on Reflection .....	313
<b>References .....</b>		<b>314</b>
<b>Appendix A: Survey forms used in Online, Street and Classroom .....</b>		<b>327</b>
<b>Appendix B: List of Academic Search Engines and Resources .....</b>		<b>334</b>

Final word counts: 81924 words of main text

## List of Figures

Figure 1-1: Sample view of an EHR (Alvarez, 2008) .....	22
Figure 1-2: Examples of content for the three dimensions in which EHRs exit (Stead <i>et al.</i> , 2005) .....	24
Figure 2-1: Canada Health Infoway architecture utilized in the Health Information Access Layer (HIAL).....	43
Figure 2-2: Breakdown of Health Expenditure.....	44
Figure 3-1: Logical view of 3P relationship in the sharing and control of information.....	72
Figure 3-2: Quantitative survey framework for patients.....	75
Figure 3-3: Qualitative survey framework for patients.....	76
Figure 3-4: Focus group discussion framework for health service providers....	77
Figure 3-5: Key informant interview framework for payers. ....	78
Figure 3-6: Invitation card for online survey .....	82
Figure 3-7: Types of findings from a Triangulation mixed method design.....	91
Figure 4-1: Qualitative survey framework for the patient. ....	100
Figure 4-2: Overall survey result of the CFIP dimensions .....	114
Figure 4-3: Percent Frequency for NOP .....	116
Figure 4-4: Percent Frequency for NOU. ....	118
Figure 4-5: Percent Frequency for NSI.....	120
Figure 4-6: Percent Frequency for NUS. ....	121
Figure 4-7: Percent Frequency for EUA .....	124
Figure 4-8: Percent Frequency for DPU. ....	125
Figure 4-9: Percent Frequency for PUA .....	127
Figure 4-10: Frequency in percentage for ARC .....	129
Figure 4-11: Percent Frequency for NSA. ....	131
Figure 4-12: Percent Frequency for CET.....	133
Figure 4-13: Frequency in percentage for VAI.....	134
Figure 4-14: Percent Frequency for BGI .....	137
Figure 4-15: Percent Frequency for BMI.....	139
Figure 4-16: Percent Frequency for MIC.....	141
Figure 4-17: Percent Frequency for TTD. ....	143
Figure 4-18: Concerns of Error by career stage cluster .....	149

Figure 4-19: Concerns about improper access to data by career stage cluster	151
Figure 4-20: Concerns about the secondary use of data by career stage cluster. .....	153
Figure 4-21: Concerns of a collection of data by career stage cluster .....	154
Figure 4-22: Frequency in percentage for SSWC.....	159
Figure 4-23: Frequency in percentage for SDSR . .....	161
Figure 4-24: Frequency in percentage for SDFL .....	163
Figure 4-25: Frequency in percentage for SDWC .....	164
Figure 4-26: Frequency in percentage for SDWE .....	166
Figure 4-27: Frequency in percentage for SCDP.....	167
Figure 4-28: Frequency in percentage for DSP .....	169
Figure 4-29: Frequency in percentage for WIW .....	170
Figure 4-30: Overall survey result of the CFIP dimensions. ....	172
Figure 6-1: shows the online homepage of eCHN.....	238



## List of Tables

Table 2-1: Health Expenditure Summary, by Province/Territory and Canada, 2014 (CIHI 2014).....	45
Table 3-1: Published benefits statements from EHR initiative.....	87
Table 4-1: Description of the three samples of the same survey questionnaire.	97
Table 4-2: Structure of the questionnaire and a brief description of the variables .....	99
Table 4-3: Modulating and response variable with a brief description .....	100
Table 4-4: Correlation of DSP among the other four variables .....	106
Table 4-5: Convergent validity of this study using Cronbach's Alpha .....	107
Table 4-6: Variables used in the four CFIP dimensions .....	110
Table 4-7: ANOVA result indicated that the three samples could not be combined into one sample. ....	111
Table 4-8: ANOVA result indicated that street and online samples could be combined.....	112
Table 4-9: Meaning of variables in collection dimension. ....	113
Table 4-10: Illustration of calculating the dimension means using “dummy” numbers.....	113
Table 4-11: Meaning of variables in CFIP secondary use.....	116
Table 4-12: Result of the 5-point Likert scale on NOP secondary use.....	116
Table 4-13: Result of the 5-point Likert scale on NOU secondary use.....	118
Table 4-14: Result of the 5-point Likert scale on NSI secondary use. ....	119
Table 4-15: Result of the 5-point Likert scale on NUS secondary use.....	121
Table 4-16: Meaning of variables in CFIP Improper access. ....	123
Table 4-17: Result of the 5-point Likert scale on EUA in improper access. ...	123
Table 4-18: Result of the 5-point Likert scale on DPU in improper access. ...	125
Table 4-19: Result of the 5-point Likert scale on PUA improper access. ....	127
Table 4-20: Meaning of variables in CFIP error.....	129
Table 4-21: Result of the 5-point Likert scale on ARC error of information. .	129
Table 4-22: Result of the 5-point Likert scale on NSA error of information. .	131
Table 4-23: Result of the 5-point Likert scale on CET error of information...	132
Table 4-24: Result of the 5-point Likert scale on VAI error of information. ..	134
Table 4-25: Meaning of variables in collection dimension. ....	136

Table 4-26: Result of the 5-point Likert scale on BGI in the collection.....	136
Table 4-27: Result of the 5-point Likert scale on BMI in the collection. ....	138
Table 4-28: Result of the 5-point Likert scale on the MIC in the collection. ..	140
Table 4-29: Result of the 5-point Likert scale on TTD in the collection.....	142
Table 4-30: Age group distribution and mapping to career stage.....	144
Table 4-31: Results of age group distribution.....	145
Table 4-32: Results of the age group in CFIP error dimension. ....	149
Table 4-33: Results of the age group in CFIP improper access dimension. ....	151
Table 4-34: Results of the age group in CFIP secondary use dimension. ....	152
Table 4-35: Results of the age group in CFIP collection dimension. ....	154
Table 4-36: Result of the four CFIP dimension by gender.....	156
Table 4-37: Frequency table for scenario SSWC. ....	159
Table 4-38: Frequency table for scenario SDSR. ....	160
Table 4-39: Contingency table for scenario SDFL. ....	162
Table 4-40: Contingency table for scenario SDWC. ....	164
Table 4-41: Contingency table for scenario SDWE. ....	165
Table 4-42: Contingency table for scenario SCDP.....	167
Table 4-43: Result of the 5-point Likert scale on DSP – Provider can keep data secure. ....	169
Table 4-44: Result of the 5-point Likert scale on WIW- Willingness to give information.....	170
Table 6-1: Interview questions.....	234

## **Abstract**

The University of Manchester  
Roy K. Ng  
Doctor of Business Administration

Privacy and Efficacy of Electronic Health Records (EHRs): A Triangulation  
Study in Ontario, Canada

2018

Patient health information kept in an Electronic Health Record (EHR) aggregates a patient's data across a specially designed health information network to produce a holistic view of their medical care. EHR systems are associated with inherent risks such as data is in electronic forms, sent across a network, accessed at multiple locations and viewed by people who may not have any relationship with the patient. Service providers traditionally controlled the access to their patient's information but are now transferred to and controlled by the EHR system. The literature shows that patients have concerns about unauthorized access to their private and sensitive health information, unlawful secondary use of this information and possible digital errors. They are also concerned about exposure resulting in social embarrassment or loss of insurance benefits.

This thesis addresses the research question: "What are stakeholder's attitudes and the perceived risks surrounding the sharing of private and sensitive health and personal information with healthcare providers and potentially having the information distributed across the health system?" In answering this question, the author framed the research in the context of the EHR system and identified Payers Patients and Providers (3Ps) as groups that interact to influence attitudes and concerns towards privacy. The author deploys a mixed methodology by using triangulation with quantitative, qualitative data collection, across time and location. The recognized "Concerns For Information Privacy" (CFIP) model to ground the topics for surveying patient's attitude towards EHR was used.

Key findings include: (a) Patients have genuine privacy concerns. (b) Service providers have similar privacy concerns about their private notes and observations to be inputted and made available in an EHR system. (c) Both groups may exercise countermeasures to protect their private information in the EHR system. (d) Payers consider patients as secondary stakeholders in the EHR system even though the patient is the legal owner and has control of their medical information. (e) Payers believe that technology protection of privacy is sufficient but many breaches are caused by humans and protection cannot prevent these events from occurring. (f) Countermeasures reduce the efficacy of the EHR that should be a patient-centric system for the benefits of patients.

The contribution of this research is a triangulation study that produces strong validation of the collected data and hence provides findings from a critical realist perspective in the understanding the underlying forces resulting in privacy concerns for patients and healthcare providers.

## **Declaration**

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

## **Copyright statement**

The author of this thesis (including any appendices and/or schedules to this thesis) owns certain copyright or related rights in it (the “Copyright”) and s/he has given The University of Manchester certain rights to use such Copyright, including for administrative purposes.

Copies of this thesis, either in full or in extracts and whether in hard or electronic copy, may be made **only** in accordance with the Copyright, Designs and Patents Act 1988 (as amended) and regulations issued under it or, where appropriate, in accordance with licensing agreements which the University has from time to time. This page must form part of any such copies made.

The ownership of certain Copyright, patents, designs, trademarks and other intellectual property (the “Intellectual Property”) and any reproductions of copyright works in the thesis, for example graphs and tables (“Reproductions”), which may be described in this thesis, may not be owned by the author and may be owned by third parties. Such Intellectual Property and Reproductions cannot and must not be made available for use without the prior written permission of the owner(s) of the relevant Intellectual Property and/or Reproductions.

Further information on the conditions under which disclosure, publication and commercialisation of this thesis, the Copyright and any Intellectual Property University IP Policy (see <http://documents.manchester.ac.uk/display.aspx?DocID=24420>), in any relevant Thesis restriction declarations deposited in the University Library, The University Library’s regulations (see <http://www.library.manchester.ac.uk/about/regulations/>) and in The University’s policy on Presentation of Theses

## **Acknowledgements**

Thank you to The Information Systems Audit and Control Associations (Toronto Chapter) in providing a research grant for this project.

I would like to express my most profound appreciation to my primary supervisor and my mentor, Dr. Rick Audas for the valuable advice and support during my journey of learning and discovery.

Thank you to my co-supervisor, Dr. Lawrence Benson for the many suggestions and support.

I would like to express appreciation to my brother, Mr. Geoffrey Ng, for the many business and engineering discussions, encouragement, and advice.

With great appreciation and thank-you to my wife, Christine, who has given me support and encouragement.

## **Dedication**

I would like to dedicate this thesis to my parents, Mr. Philip Ng and Mrs. Irene Ng, who had taught me the value of perseverance and responsibilities in taking on life's challenges.

## **In Memories**

To my beloved brother, the late Mr. Danny Ng who had given me the opportunity to walk the path together with him in facing life's challenges.

.

To my dear classmate, the late Mr. Lawrence Ho, you have shown me how to face life's challenges with courage and tranquility.

## Preface

As per suggestion from the Presentation Thesis Policy, Section 4.2. (b) p.8, below is the author's research experience and conference papers and book chapter written.

### The Author

Roy Ng, is a Research Fellow with the Privacy and Cyber-Crime Research Institute and a former Assistant Professor at Ryerson University, an AACSB university in Toronto, Canada. He received his Bachelor of Business Administration degree and a Bachelor of Arts (Economics) degree both from York University, Toronto and a Master of Business (Information Technology) degree from Royal Melbourne Institute of Technology (RMIT), Melbourne, Australia.

### Peer-reviewed papers and book chapter while with The University of Manchester

Ng, R. & Ng, C., (2012). Towards a Framework of Information Assurance in the Protection of Patient's Privacy in Electronic Health Record (EHR), *International Conference on Management and Service Science*, Shanghai, China. August 10-12, 2012. IEEE

Ng, R. & Dong, L. (2008). An Information Assurance Framework on Trusted Autonomic Communications. Conference Proceeding, *International Symposium on Electronic Commerce and Security 2008 conference*, Guangzhou China, August 3-5, 2008. IEEE

Ng, R. & Dong, L. (2008). A Case Study: The Deficiency of Information Security Assurance Practice of a Financial Institute in the Protection of Privacy Information, Conference Proceeding, *The First IEEE International Conference on Ubi-media Computing*, July 31-August 1, 2008

Ng, R. (2008). A Holistic Approach to Information Security Assurance and Risk Management in an Enterprise, in Gupta, J. & Sharma, S. (eds) *Handbook of Research in Information Assurance and Security*, USA, IGI Global, Ch. 5 pp 42-52.

# **Chapter 1 Introduction**

## **1.1 Introduction**

Health authorities around the world are implementing Electronic Health Records (EHRs) systems. The benefits of improving the quality care of patients, control the current rapidly increasing cost of healthcare by deploying EHR system are well documented (Thakkar, 2006, Canadian Health Infoway, 2006). However, the utility of such a system will be compromised if patients withhold private and sensitive health information. This research examines the issues of information sharing in the context of the patient privacy concerns in the EHR system in Ontario, Canada.

This chapter provides a broad overview of the research issues. The introduction poses and explains the research question and the relevance of the study, setting it in a broader context of the current debates and challenges in healthcare delivery and growing concerns about privacy and data access of the Electronic Health Record (EHR).

## **1.2 Background**

The purpose of this thesis is to study patients' risk attitudes and concerns regarding their private health information designed to be held in the EHRs that are currently being built and partially implemented in Ontario, Canada.

The rapidly increasing cost of healthcare, the global concerns of health-related pandemics and growing worry about the impact of chronic diseases have accelerated the demand for the modernization of healthcare information

systems. The benefits seen in the prior experience of processing of e-commerce applications has led to the early adoption of electronic health records system. The result has proven to increase the effectiveness and efficiency of better healthcare management as compared to paper-based health record systems (Barsauskas *et al.*, 2008).

The traditional health records of a patient are on paper or in an image format of laboratory results that are usually stored on a paper inside a file folder in the name of the patient. Copies of these papers are held by different healthcare service providers (hereafter called providers), such as family doctors, radiologists, pathologists, or pharmacists. These folders of partial or incomplete patient records contain medical histories, diagnoses, observations, and drugs used by the patient in a paper format are segregated and kept by individual providers. Patient health information that is stored in paper format is harder to access, analyze, and share than when it is in electronic form (Hoyt and Yoshihashi, 2014; Webster T, 2017).

EHR systems promise many benefits but require electronic forms and standardization with the capability of transmitting over computer networks for sharing and remote access to EHR data. Global deployments of EHRs are designed with various configurations to achieve success. These arrangements include top-down approach, bottom-up approach or hybrid approach in implementation with top-down government specifications, and local expertise for bottom-up implementation and realization of benefits (Eason *et al.*, 2012; McGinn *et al.*, 2011). In Canada, the configuration is national government top-down specification for standardization and interoperability and funding with each province performing the detailed design and implementation for customized requirements and benefits unique to the province (Gagnon *et al.*, 2019).



### 1.3 The Definition and the Concepts of Privacy

There are many different definitions of privacy. Each has a slightly different emphasis. In Oxford Learner's Dictionaries, Privacy refers to "The state of being alone and not watched or disturbed by other people" or "the state of being free from the attention of the public" (Oxford Learner's Dictionary, 2017).

In Cambridge Dictionary, privacy refers to "Someone's right to keep their personal matters and relationship secret" or "the state of being alone" (Cambridge Dictionary, 2017a)

In Merriam-Webster Dictionary, it defines privacy as "the quality or state of being apart from company or observation: seclusion" or "freedom from unauthorized intrusion *one's right to privacy*" (Merriam-Webster Dictionary, 2017)

Through talking with participants in this research, the author has observed that different people have different emphasis and intensity towards privacy. Some focus on being left alone and others stress on their right to keep their personal matters and relationship secret. In this thesis, the author defines the privacy in EHR in the following way: Privacy refers to the data and information in the Electronic Health Records that is deemed to be of private and sensitive nature. To the patient and that such data should not be available to "unauthorized third party" or those who are not in the immediate circle of care. In the case of service provider, privacy is those personal notes and data that the service provider entered into the EHR for his/her own reference in the future but do not wish to be accessible by any unauthorized person. This definition used by the author also upheld two common emphases of "being left alone" and "the rights to keep the personal matter secret." These emphases can be further elucidated with the concepts of privacy.

### 1.3.1 The Concepts of Privacy and its Extension to Electronic Health Records (EHRs)

According to Flaherty (1991) in On the Utility of Constitutional Rights to Privacy and Data Protection:

*PRIVACY IS LIKE freedom: we do not recognize its importance until it is taken away. In that sense, it is a personal right that we assume we have yet take for granted until something or someone infringes on it. Privacy, like freedom, is difficult to define except in the negative. (Flaherty 1991, p 831)*

The following relevant concepts in privacy help to set the context of the discussion in this thesis. Further discussion of these notions can be found in the chapter on literature review, and the analysis chapter in this thesis.

Concept 1: Entitlement to be let alone: Privacy encompasses the connotation of a person's affairs and information not to be mentioned. This entitlement also includes the prerogative to make secrecy or keep from the sight of information from unauthorized others (Warren & Brandeis, 1890; Thomson, J., 1975). In electronic health records, private information of a patient is to be let alone (Harman *et al.*, 2012).

Concept 2: Expectation or ability to limit others from accessing one's personal information. In doing so (Nordgren, 2015), one would have the capacity to control (Solve, 2008) who can access the information either when they provide the source information or expect the custodian of information to be able to regulate the retriever of information. According to Charles Fried (1968, pp. 482), "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves." In privacy law in Canada, The Personal Information Protection and Electronic Documents Act in Canada restricts the access and collection of personal information. (Minister of Justice, 2017).

Concept 3: Non-exposure of personally identifiable information (PII): Very often, one of the primary requirements of privacy is to restrict the part of the

identification information of a person to be seen or accessed by others without justified cause or authority. Such restrictions help to prevent the risk of harm coming to the owner of the information. In the context of EHRs, the patient is the legal owner of the contents of the information described in the records. Such ownership in EHR was affirmed by the Supreme Court of Canada in its decision of *McInerney v, MacDonald*, a case in 1992 by Judge La Forest *et al.*, (1992).

Concept 4: Privacy requirement is a very individual matter: It is the author's extrapolation from literature (more discussion in chapter 2) that the intensity and level of privacy concerns of a patient and his/her decided action of protection is a very personal one. It is based on one's perception of the privacy risk and requirement to countermeasure (remedy) the impact. Some people are less worried about the exposure of their private information than others who are most concern about their private information is being exposed. This concept is also peripherally (marginally) discussed in Xu *et al.*, (2001, pp. 798) paper in "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances".

Concept 5: Privacy risk reduction in EHR by using countermeasure: Countermeasure is defined as "an action taken against an unwanted action or situation" (Cambridge Dictionary, 2017b). The author of this thesis borrowed the concept of countermeasure in information security protection to privacy protection. Countermeasure in privacy protection in the context of EHR, according to the author's definition, is that the owner of the information initiates an action to counter the anticipated or actual adverse effect resulting from a breach of privacy caused by unauthorized people accessing the private information in an EHR system. This privacy exposure includes the poor design and insufficient privacy protection procedure of an EHR system. By initiating an action in countermeasure, the owner of the data, therefore, reduces the risk and impact of such exposure. The owner of information also includes service providers who own part of the information in the electronic health records when entering their diagnosis information or personal notes into the EHR.

## **1.4 The Many Names of EHR and Definition Used in This Research**

In the implementation of EHR, different countries and organizations have different names and emphasis on the use of Electronic Health Records and therefore, refer the term EHR by similar yet non-identical names. Precise definitions of EHR may reduce confusion. It is essential to distinguish these terms and defines what EHR is. According to Professor Hammond, from Duke University, in his presentation at the Eurorec 2002 Conference in Berlin, the following terms are closely related to EHR and can sometimes be used interchangeably with EHR. They are AMR CPR, EMR, EPR, CBPR, PRMI, PHR, EHCR, and ICRS (Hammond, 2002). A lookup of these acronyms using the Acronym Finder (TAF, 2010) reveals the following abbreviations:

- AMR (Automated Medical Record),
- CPR (Computer-Based Patient Record),
- EMR (Electronic Medical Record),
- EPR (Electronic Patient Record),
- CBPR (Computer-Based Patient Record),
- PRMI (Partial Response Maximum Likelihood),
- PHR (Personal Health Record),
- EHCR (Electronic Health Care Record) and
- ICRS (Integrated Care Records Services)

Among all names used in the above, the three most commonly used one are EHR, EMR, and PHR. EHR and EMR are also used and sometimes confused by users in Canada (CHI, 2011). There are many definitions of these terms including an “official” definition from the International Standard Organization (ISO-TIC20514, 2004). However, of all the explanations offered for the above three terms, the highest clarity is:

An EMRS automates aspects of clinical practice, such as placing a care provider order, recording a clinical note, or capturing administrative functions such as scheduling and billing. A patient's electronic medical record (EMR) is generated as a by-product of these clinical and administrative duties. It often lives within the particular EMRS that created it and is unique to that system. In that case, the EMR's meaning is clear only to that specific EMRS since the record is constructed with terminology and data structures particular to that system. (Stead *et al.*, 2005, p.114)

EHR refers to any information in electronic form about a person that is needed to manage and improve their health or the health of the population of which they are a part of (Stead *et al.*, 2005). PHR refers to a personal electronic collection of health information. The PHR includes patients' records of their progress and changes they have made in therapy plus their electronic copies of information from their providers (TAF, 2010).

The above three terms are used interchangeably by the public (Hammond, 2002). However, these terms are distinctly different from EMR, which is used mostly within service provider establishments such as hospitals to track and log patient conditions and progress. EHR is used by healthcare providers to help deliver quality care services to patients by the government in standardizing the healthcare record and healthcare management. PHR includes a patient's own personal collections of their medical condition, data, and notes and is patient-centric.

In this research study, the author uses the definition from Canada Health Infoway (CHI, 2006) of an EHR as a longitudinal collection of the health information records of a patient and is stored in an electronic format within a computing facility and can be easily transmitted and shared among many providers. These electronic records accumulate the medical history of the patient and treatment each time a patient visits a service provider or taking a medical test at a laboratory. The EHR contains patient demographics,

problems, vital signs, medications, progress notes, past medical history, immunizations, laboratory data, and radiology reports (HIMSS, 2011).


<ul style="list-style-type: none"> <li>• Help</li> <li>• Logout</li> </ul>	<b>Patient Details</b>			<b>GP Details</b>		
	 <b>GME0000 Smith, Caroline</b>			<b>Name:</b> Jones, Evans	<b>Phone:</b> 333-465-5545	<b>Address:</b> 11 Terrence Ave., Edmonton, AB T4Y 8U9
	<b>Other Healthcare Providers</b>			<b>Name</b>	<b>Disp.</b>	<b>Last Encounter</b>
	<b>Sex:</b> Female <b>DOB:</b> 1940/01/01 <b>Next of kin:</b> John Smith			<b>Next encounter</b>	<b>Right of Access</b>	
	<b>Alerts</b> Allergies – Sulfa Drugs • Pap smear due • Td due • A1C above target			<b>Medications</b>	<b>Prescriptions</b>	<b>Last Filled</b>
<b>Patient Record</b> <ul style="list-style-type: none"> <li>• Summary</li> <li>• Lab Results</li> <li>• Diagnostic</li> <li>• Images</li> <li>• Details</li> <li>• Notes or Comments</li> </ul>	<b>Diagnosis</b>			<b>Date</b>	<b>Medications</b>	<b>Prescriptions</b>
	Hypertension 11/1989 Ongoing Diabetes 05/1996 Ongoing Coronary Artery Disease 02/2002 Ongoing Fasting lipids 12/2005 Exercise stress test 1/2005 Coronary angiogram / Cellulitis 02/2005 Resolved Cholecystectomy 05/1981 Resolved Cesium section 01/1967 Resolved			<b>Medications</b>	<b>Prescriptions</b>	<b>Last Filled</b>
				<b>Encounter History</b>		
				<b>Date</b>	<b>Facility</b>	<b>Speciality</b>
				<b>Clinician</b>	<b>Reason</b>	<b>Type</b>
<b>Immunizations</b>				<b>Diabetic Indices</b>		
				<b>Type</b>	<b>Value</b>	<b>Most Recent</b>
				<b>Influenza</b>	<b>A1C</b>	<b>12/2005</b>
				<b>Pneumovax</b>	<b>LDL</b>	<b>12/2005</b>
				<b>Twinrix</b>	<b>BP</b>	<b>02/2006</b>
				<b>Td</b>	<b>Urine</b>	<b>08/2005</b>
					<b>Microalb</b>	<b>05/2005</b>
					<b>Eye Exam</b>	<b>05/2005</b>
					<b>Home Gluc</b>	<b>01/2006</b>
					<b>(average)</b>	<b>7.4</b>

Figure 1-1: Sample view of an EHR (Alvarez, 2008)

Figure 1-1 shows a sample view of an EHR presenting various information about a patient's medical and healthcare history to be implemented in Ontario, Canada. A role-based access system with different viewing privileges of data has been designed. For example, a doctor will see much more information about a patient than a medical secretary that schedules appointments. As shown in Figure 1-1, information in the EHR can be very comprehensive and can help a healthcare service provider to provide efficient diagnoses and treatment decisions. It is this holistic view of information that creates vulnerabilities in privacy risk and security exposures of sensitive information of the patients. For this same concern of privacy risk, American patients have taken countermeasures to disaggregate the collection of health information to avoid a comprehensive collection of their medical information in EHRs.

## **1.5 Three Different Stakeholders Using Different Domains in EHR**

To understand the patients' privacy concerns in EHR and to increase the validity of the findings in this research study, the author takes a holistic approach by examining the three stakeholder groups. They are patients, providers, and payers (hereafter referred to as the 3Ps). Patients have concerns about protecting their private information in an EHR system. Providers are healthcare service providers. They need comprehensive, accurate and complete information to provide quality care. Payers in this context are managers and decision makers from the Provincial Ministry of Health, Regional Health Authorities and eHealth Ontario, who are responsible for the EHR implementation. They are attempting to control health costs while increasing value such as quality care and time efficiency for patients.

According to Stead *et al.*, (2005), EMR and PHR have shared data (overlapped data) and their non-shared data. In the Canadian case, the author suggested that data in the EHR also includes some part of data in EMR. PHR is more popular in the United States than in Canada. Theoretically, PHR is a superset of both EMR and EHR. In practice in Ontario, PHR is still in a stage of infancy and start gaining attention with some private, commercial organizations providing patient self-tracking logging capabilities and storage of information over the Internet for remote access by healthcare providers (Shaw, 2016). Also, in spring 2016, a large medical laboratory chain called "Dynacare" launched a product called "Dynacare Plus." Patients can now use this service to access their lab results and receive a clear explanation of each item of their test result with tracking over time (Biospace, 2015; Dynacare, 2016). Figure 1-2 from Stead *et al.*, (2005) shows the three dimensions (domain) of the health information data used in EHR.

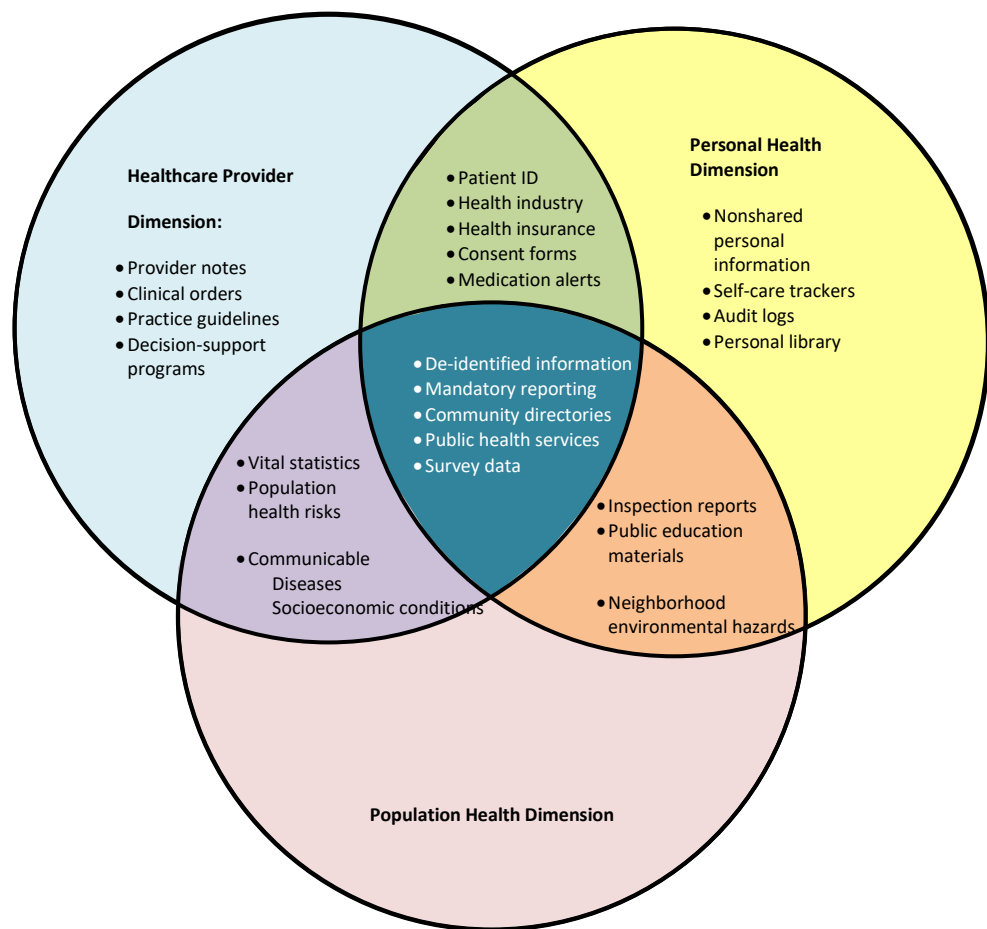


Figure 1-2: Examples of content for the three dimensions in which EHRs exit (Stead *et al.*, 2005)

The author believes that these three dimensions are useful in framing the context of this study onto the three different groups of stakeholders (3Ps) of EHR. Each group utilizes one of the three dimensions. The "patient" group uses the "personal health" dimension to monitoring their health. Health service "providers" (such as family doctors, pathologists, cardiologist, and pharmacists) use the healthcare provider dimension to assess and make medical decisions when caring for patients. The "Payers" (Government health ministry or regional health authorities) utilize the population health dimension for public health management. These three dimensions in Figure 1-2 depicts the theoretical perspectives in determining the research questions in this thesis relating to the three primary stakeholder groups (3Ps). In this research, patient attitudes and concerns are the focus of the study, the data, and insights derived from



interviews with payers, and focus group discussion with providers is used for cross-examination (triangulation methodology) to explain and understand patient concerns. It is essential that this research study examines all three stakeholders (3Ps) groups.

## **1.6 Pan-Canadian Implementation of EHR**

In 2001, the Federal government created an organization, Canada Health Infoway (CHI), which is funded at the federal level. Its primary task is to accelerate and standardize the development and interoperability of EHRs in Canada. CHI is a national level, independent and not-for-profit organization whose members are Canada's fourteen federal, provincial and territorial Deputy Ministers of Health. CHI has received 2.1 billion dollars (Office of Auditor General of Canada, 2009) in capital for about 370 e-Health projects across Canada, working with the provinces and territories. As of 2011, 1.6 billion dollars has been spent on about 280 e-health projects across Canada. (McLeod, 2013 p.1).

In 1990, Ontario Ministry of Health started planning for EHR implementation, and in 2002, the Ministry created a provincial level organization called "Smart Systems for Health Agency (SSHA)." According to the Ontario Auditor General, Jim McCarter (2009), the mission of SSHA was to create and oversee a secure electronic network and the connection to the medical community to this network. SSHA is to provide communication infrastructure and the ministry designs EHR software and database to run on SSHA's secure system. However, McCarter has assessed that SSHA had not been able to provide mandatory performance reporting of the agency's operations. Funding of SSHA had increased from \$13.5 million to about \$213 million over nine years. This funding has contributed mainly to the building of infrastructure for EHR. As a result of overspending of SSHA (800 million dollars with unsatisfactory progress), the Ontario Ministry of Health created eHealth Ontario in 2008 to

take over both SSHA and the Ministry's EHR initiatives. This arrangement provided a better focus, improved accountability and an effective integration in the implementation of EHR in Ontario (McCarter 2009).

The approach in implementing the EHR project, from CHI to each province in Canada, is a shared responsibility (Office of Auditor General of Canada 2010). CHI provides funding for approved EHR projects, and the ownership and implementation of provincial EHRs are under the jurisdiction of each province. In Ontario, Ontario Ministry of Health is responsible for overall provincial strategy while eHealth Ontario is responsible for implementation and the deployment of information communication technology (ICT) and software application design of EHRs to improve patient care, safety and records access in support of the government's health strategy. According to eHealth project plan, eHealth Ontario is mandated to have electronic health records in place for Ontarians by 2015 (eHealth Ontario, 2015). According to CBC News and eHealth Ontario's progress report online, as of Dec 28, 2015, only two-thirds of Ontario have digital medical files (CBC News, 2015;).

Recognizing the need for national interoperability of EHR systems, CHI started the mission by first establishing an EHR blueprint to provide guidance, decision-making and standards adoption among the provincial healthcare systems (CHI 2006). The aim in CHI is to allow some flexibility among the provinces to establish their EHR systems that can be customized to their needs and yet in compliance with the national standard of interoperability. By sponsoring the funding of the provincial initiative on behalf of the federal government, CHI provides financial incentives and project guidance to each province. Other notable work being completed by CHI includes creating standard collaborative functions by setting up workgroups. For example, "standard workgroup no. 8" is in charge of developing Pan-Canadian Privacy and Security Architecture for EHRs.

## **1.7 Patient Concerns About Their Privacy in EHR**

There are expectations from patients on the published benefits for EHR deployment that include improved quality of healthcare from providers, proper administration, and privileges of fee concessions from Payers (government). However, the comprehensive view of patient medical histories and detail digital results of treatment available in an EHR is considered by patients to be private and sensitive information (New London Consulting, 2011; Smit. et al., 2005). It is hypothesized in our research study that patients also have concerns about protecting their private and sensitive information in the Ontario EHR system to avoid embarrassment and loss of career opportunities or insurance benefits. Providers need comprehensive, accurate and complete information to provide effective and efficient medical diagnoses and practices in the delivery of quality healthcare. Payers in this context are provincial ministries of health and regional health authorities and eHealth Ontario. They are attempting to control the rapidly increasing healthcare costs while increasing value, such as quality of health care and time efficiency, in addition to managing and controlling chronic and epidemic diseases in public health.

Research from the US and New Zealand (Ash, 2004; Fernández-Alemán. *et al.*, 2013), suggested that there are patients' privacy concerns in EHRs. The author is interested in finding out if there are any similar concerns in Ontario. The EHR is being implemented in progressive stages. Payers and providers may benefit by understanding the attitudes of patients towards risk in their concerns for their privacy. This research can help in the design and implementation of controls in the information assurance for the protection of private information of the patients.

## **1.8 Will This Happen in Canada?**

In a US national survey of 2200 Americans released in January 1999 (California HealthCare Foundation, 1999), one in five persons believed that their personal health information had been misused without their knowledge or consent. More striking was that one in six persons engaged in some form of privacy-protective behavior to shield themselves from what they considered harmful and intrusive uses of their health information. Examples include withholding information from their healthcare providers, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and in the most extreme cases, avoiding health care altogether.

With the risk-averse attitudes and the actions demonstrated by US patients in dealing with EHRs, it is prudent to research the view of patients in Canada to determine whether Canadian patients have similar concerns with the private information that is held in the EHR system. Any level of privacy concern will likely be increased as EHRs go online, and health information travels faster and is available ubiquitously from provider to provider and institution to institution. With the potential for patients to hold back medical information due to privacy concerns, this could result in providers be constrained in their ability to provide effective and efficient treatment. Such holding back of information may create "wastage" of medical resources such as unnecessary laboratory tests being ordered; time and suffering by patients due to retesting and possible adverse health effects due to additional testing. An example of adverse health effect due to retesting may include exposure to radiation through multiple duplicative diagnostic imaging requests (Griener, 2015, Shellock and Spinazzi, 2008) or radiation from diagnostic imaging may carry some risk to patients. In the opinion of the author, patient's intentional wastage of medical resources is an abuse of the universal and free healthcare system in Canada. An example is when patients see multiple doctors for the same problem but intentionally giving inaccurate or incomplete information due to their privacy concerns.

It is hypothesized by the author that patients perceive the existence of risk in the protection of their private and sensitive information in the EHR systems. For example, EHR systems by its principles of design provide a collective sharing of patient health information to be viewed and accessed by many healthcare providers. The perception and attitude towards this risk may cause patients to be less willing to share vital health information thus, potentially compromising the utility of the EHRs and the own patient well-being. This study is intended to understand the patient attitudes toward privacy protection of the EHRs.

Patient information collected by EHR system can be at risk when used by service providers or other authorized administrators in Ontario when they have no relationship with the patient but are allowed to access the data by the EHR system because of their roles in the system.

The perception from patients with an organization's ability (such as eHealth Ontario) to keep secure and private information in real control affects the trust and participation of patients and service providers in the EHR system (Xu *et al.*, 2001). This patient's perception is of particular importance to patients whose very private and sensitive health information is stored in various local providers' servers but can be aggregated into an EHR for viewing via the health information network with the EHR system.

## **1.9 The Implication of Privacy and Security Issues with EHR**

EHR, by design, contains sensitive and private information about patients' health conditions. Most people will consider their status of health, illness, and treatment as a personal and private matter. The author perceived that there are numerous potential issues and privacy concerns. These issues are:

(1) With the information in an electronic form, patients cannot readily see their health information without using a computer. In contradiction, patients can view their health information in records in hard copy quickly when they ask for a

copy of their health record in the paper form. Computer terminal and knowledge of computer technology must be learned before a patient is comfortable in accessing their health information electronically such as accessing Dynacare Plus offered by Dynacare. With the above difficulties described, this creates alienation and mistrust of the information obtained due to the awareness of the common breach and compromise of a communication network and computing facilitates as similar incident reported by Ontario Privacy Commissioners (detailed description in Chapter 2). The author perceives that older patients may have less exposure and aptitude in using computer systems, yet their chances of being ill are higher than that of younger patients, therefore more EHR gathered on their health condition.

The nature of digital information in EHR poses concerns about data confidentiality and integrity. Unlike paper records containing handwritten information, digital information can be easily copied, deleted, and altered without the detection of the owner or custodian. Numerous incidents and security breaches have been reported, and such events have exacerbated patient worries. It also created doubt toward the trustworthiness of the integrity and privacy protection of their health data.

(2) Network communication technology in EHR implementation has provided connectivity and ease of use to users through the integration of many separate networks over a Health Information Access Layer technology. Without proper design of privacy and security protection in EHR, it can be easily exploited by information hackers or even by authorized users

(3) In all provinces in Canada including Ontario, health care is universally available to all residents of that province. Ontario Health Insurance Program (OHIP) is the universal healthcare program in Ontario. Employees pay their OHIP subscription premium via mandatory payroll deduction, and no premium is required for residents with little or no income. The government, in turn, pays for the cost of patient's healthcare service directly to the service providers. Almost all eligible residents and service providers use the OHIP program in Ontario. The EHR system receives patient's EHR data from service providers.

As it is a universal program, everyone in the OHIP system is subjected to the security and privacy risks of the EHR systems.

In the USA, the healthcare expenses are under the Medicare program for people with low incomes, but eligibility also depends on meeting other requirements based on age, pregnancy status, disability status, other assets, and citizenship. Medicaid provides coverage for elderly and certain disabled Americans. Even with the Affordable Care Act took place in 2010; there are still a significant number of people who are underinsured or uninsured. Schoen *et al.* (2014) on her report America's Underinsured stated that:

*The analysis finds that in 2012, there were 31.7 million insured people under age 65 who were underinsured. Together with the 47.3 million who were uninsured, this means at least 79 million people were at risk for not being able to afford needed care before the major reforms of the Affordable Care Act took hold. (Schoen et al., 2014 p.ix)*

In 2016, new Internet health portals have been established by private enterprises in Canada. For example, TELUS Health created a health portal for patients to access their health information utilizing a public internet infrastructure. Although TELUS claimed that the health platform is secured and is certified by Canada Health Infoway, there is still privacy and information security risk for home-based computing equipment accessing a technology platform. (Henriksen. *et al.*, 2013).

## **1.10 Protection of Personal Health Information in Ontario**

The Office of Information and Privacy Commissioner of Ontario (IPC) was established in 1987 after the passage of the Freedom of Information and Protection Act (FIPPA) in Ontario. The work of the IPC mainly focuses on two

areas. One is the individual's right to access government institutes and institutes of higher learning that act as custodian or is in control of private information. The FIPPA provides regulations in the process of control and security of information entrusted or controlled in government institutes. Detailed rules on how the information should be collected, properly used and restrictions of disclosure, retention and finally how it should be removed for destruction. The author called it "Information Life-Cycle." The act is also concerned with the aspects of privacy and security of information. In 2012, Ontario hospitals were included as institutes under the regulation of FIPPA (The Government of Ontario, 2017).

Recognizing the risks of digital information (quickly exposed in the computer function of view, changed, copied, deleted) as e-commerce progressed, a federal privacy law, Personal Information Protection and Electronic Document Act (PIPEDA) was enacted in the year 2000 to regulate the information life-cycle. As PIPEDA identified medical records as a very sensitive personal information, two years after the inception of CHI in the building of the EHR blueprint, in 2004, the Personal Health Information Protection Act (PHIPA) was legislated in Ontario (Herrmann, 2007). The PHIPA is a direct recognition of the patient privacy. This act regulated and mandates the requirements for healthcare providers in the custody of patients' health information and listed out the rights to access and correction of the information by patients. (The Government of Ontario, 2017).

Although there has been much work done by The Office of Information and Privacy Commissioner (IPC) in identifying privacy issues, providing toolkits to the public in preventing and mitigating privacy breaches via their website, during our research study, it appears that many Ontario residents have not heard of and were not familiar with the work of IPC.



### **1.11 Research Question and Importance of This Research**

The author hypothesized that patient withholding their private and sensitive medical information from EHR creates paradoxical constraints for both themselves and service providers. It is especially true for providers who require this withheld information to deliver quality medical care. Adverse events may occur when providers are missing critical pieces of information while diagnosis and clinical decisions are being made. Unnecessary repetition of tests or verbal dialogues needed to obtain vital information for diagnosis and treatments, and this can be both costly for the payer and risky for the patient.

This research explores patient attitudes and contributing factors from providers and payer that results to patient privacy and security concerns in the sharing of their electronic health records over an integrated computer communication network among the many health service providers. It also investigates the decision of patients in their willingness and cooperation to disclose their private and health information to the health service provider.

The primary research question is: What are stakeholders' attitudes and the perceived risks surrounding the sharing of private and sensitive health and personal information with healthcare providers and potentially having the information distributed across the health system?

The focus of this research is to investigate patient willingness to provide and share private information with providers and to contrast this willingness under various stress levels regarding hypothesized health conditions. Since the EHR system is not yet fully implemented, this research is particularly important in making the findings available to the 3Ps. If the patient privacy issues are not adequately dealt with at the design or revision phase, the utility of the actual EHRs system could be significantly compromised.

EHR systems, in many cases, form part of a decision-support system (DSS) when a provider decides what treatment a patient should receive. Medical and lab results of a patient EHR will constitute the core database in such a system. Goldstein *et al.* (2002) explained that decision support systems could assemble

information for easy review, offer advice, and suggest alternatives not immediately apparent to the clinician; however, as a new technology, they can also introduce new sources of error. His group has identified the following potential sources of error or impairment in drug recommendations:

Harm to patients --- Potential harm due to medication withdrawal; Missing data leading to the recommendation of a contraindicated drug; Potential interaction of the recommended drug with another drug prescribed for the patient; Potential harm (to a patient) due to rearranging clinician priorities using the Decision Support System (DSS).

Inefficiency or error to the provider --- Inaccuracies in program inputs or program logic which could lead to erroneous recommendations; Knowledge gaps of the clinician-user that are directly relevant to the DSS recommendations; Generating false expectations on the part of the clinician-user that the system will alert them to all problems.

This research examines the information that patients consider to be private and the information that service providers need to provide effective and sensitive treatment. Also, scenario-based survey questions will also be used to assess changes in risk attitudes of patients when faced with increasing severity of their medical conditions. Progressive strengthening (toughening) of patients' action in protecting their privacy is explored.

This research study contributes in six areas: (1) A study to find out whether Ontario patients follow the same patterns as in the USA regarding patient avoidance of aggregated EHR information due to their perception of privacy violation of their personal health information. (2) An assessment of the claimed benefits of EHR published by payers (designers). (3) A quantitative measurement of whether patients will compromise their attitude of guarding and protecting their private information when their medical condition changes from normal to severe to a life-threatening situation. (4) Focus group interview is used as an assessment of providers' needs and concerns in the EHRs system. (5) An examination of potential factors influencing the efficacy of delivering the EHR system in Ontario, and (6) An exploration of other concerns related to privacy of EHR from the payers, providers, and patients.

## **1.12 Thesis Structure**

The structure of this thesis is as follows: Chapter One provided an overview and introduction of the EHRs system and the research question. Chapter Two surveys the body of knowledge using literature review formulates the research problem and refines the research question. Chapter Three discusses the theoretical framework, research methodology, and design. Chapter Four describes the results of a patient survey. Chapter Five describes the findings in the focus group discussion with providers; Chapter Six describes the results of key-informant interviews with payers and stakeholders from professional bodies. Chapter Seven provides an analysis and a discussion of the results and research findings. Chapter Eight presents a conclusion, the author's reflection of the challenges and the limitation of this investigation and closing this study with suggestions for future research.

This thesis study uses a mixed methodology with the quantitative survey, qualitative focus group discussions and qualitative key informant interviews to obtain data. Three groups of subjects are used. They are patient, service provider and payers. A triangulation design is used to cross-reference the data from the service provider and payers against the core group findings of the patient. Triangulation design helps in synthesize and increase the validity of the results.

### **1.13 Chapter Summary**

In this chapter, the author has introduced the needs of EHR from paper records due to the requirements of efficiency, better health care, control of health costs and quick assimilation of information for public health. By defining the key terms and names of EHR, analysis and discussion can be framed within the definition. The issues of digital format of EHR is introduced followed by the patient's concern about privacy. The author introduced five concepts related to privacy and borrowed the concept of countermeasure that is commonly used in information security protection. The research question is introduced with a description of how the thesis is structured.

## **Chapter 2 Literature Review**

### **2.1 Introduction**

This chapter describes the literature related to the research problem and the primary research question stated in Section 1.11. The scope of the literature review centered on the following areas: (1) The worldwide design approach and implementation of EHRs, and Canada's EHR implementation; (2) The costs and benefits of EHR that motivate the Canadian EHR project; (3) Privacy breaches in Ontario; (4) What theoretical frameworks or models have been developed in the assessment of privacy of information? (5) Have studies been done related to privacy in EHRs? (6) Gaps identified in the literature related to privacy in EHRs from scholars. This literature review and the gaps identified help formulate the research sub-questions.

The scope of the review includes an examination of the scholarly literature and discussions related to the design and implementation; costs and benefits of the Electronic Health Records (EHRs) and the breach of privacy incidents. It is the author's opinion that how the design and implementation of EHR may be significant factors that influence the patients' perception and attitude towards their concerns about privacy in EHR.

### **2.2 Conducting the Literature Review**

The literature review of this study started with defining the research question. Given the observation of the potential privacy risk in the electronic forms of health records (EHR), the research question was formed with study areas. They are (1) Patients attitude (2) privacy risks, (3) Sharing of private information (4)

with providers and (5) distribute across the health system. Once research question was formed, it was then refined into sub-questions to a significant and meaningful scope and focus. A literature review was started from a worldwide view then narrow down to the country and provincial (Ontario) level. Key search terms include patients attitude, electronic health records, risks, countermeasure, security and privacy protection, issues and lesson learned on EHR implementation, assessment models on government-led implementation programs. The search centered first on scholarly literature for the past 12 years, and government publication of EHR program blueprints, design architecture document and the benefits were reviewed and collected. Other supplemented publication included related privacy legislation, law definition, court case results and many news articles and editorials. The gaps are then identified. This help framing of the research sub-questions into the 3Ps with the scope of the privacy and efficacy of EHR as the overall framework of discussion. Appendix B shows a list of academic search engines and resources that have been reviewed for suitability and accessed to create the literature databases. A total of 754 articles and papers were collected and formed the database of the literature review in the research management software Endnote (version 7.8).

### **2.3 Worldwide Approach and Implementation of EHR**

For over a decade, many countries have undertaken research and development of EHRs into implementation projects. These projects aim to develop an infrastructure for national health information. In Europe: England (Morrison, 2010), Denmark and Finland (Ministry of Social Affairs and Health, 2010) are well advanced in EHR implementation as compared to the United States and Canada (CHI, 2009). Australia is also a leader in EHR development and implementation.

In Canada, both the provinces of Alberta and Newfoundland are at an advanced stage in EHR implementation when compared to the rest of the country. In Ontario, the EHR system is now at a stage of partial deployment. In the

following sections, progress towards implementing an EHR in various jurisdictions is described.

### Europe

According to Arnold (2007), in Europe, Electronic Health Record systems in England and Wales and Denmark are nationalized. England and Wales are one of the leaders in EHR and is at an advanced stage of implementation. They have established the EHR initiative by the National Health System (NHS) providing a Care Records Service (CRS) platform. The objective of the CRS program is to enable nationwide transfer of EHR and create interoperability of the records among providers. The EHR architecture in England and Wales uses a centralized repository with a national infrastructure. They have created an Internet patients' portal where patients can view their health records. A centralized national infrastructure can provide a higher standard of privacy and security protection, as standardized process and procedure can easily be maintained. However, the implication of allowing Internet access to health information portal is the facilitation of hackers exploiting the health information system and, therefore, reducing the level of protection achieved with a centralized infrastructure. It is commonly known that hackers place viruses or "Trojan" spyware to collect sensitive personal information and passwords. The ability of key logging on a computer when a patient is accessing EHR information exposes private and sensitive information.

Denmark formed the National EHR Organization to run the government funded EHR program and established the interoperability standard for EHR. Canada followed the European countries to ensure potential international interoperability by such standards (Stroetmann, 2011).

France and Sweden continue to move towards a government-funded EHRs with a national strategy for an EHR system, while Germany and the Netherlands are still in the process of formally committing to this model (Arnold, 2007).

In Norway, research is being done to decide how to implement a national EHR. The EHR system in Norway is decentralized. The Norwegian University of Science and Technology (NTNU) established the Norwegian EHR Research

Centre (NSEP) in 2003. The primary activity of the Research Centre is the development of research and knowledge in support of EHR deployment in the health services. Ninety-eight percent of clinicians have an EHR platform with the Norwegian Health Network as the infrastructure for EHR implementation (Doupi, 2010).

In the Netherlands, local and regional electronic health records are already in use. However, they are not regulated by any specific legal provisions. The proposal currently under discussion in the Dutch Senate intends to introduce a system for a countrywide-shared EHR. It will only aim at data processing within the Netherlands. The interoperability and sharing of health data by providers have not yet been achieved. Similar to a database system, the data intersection is the core element of the EHR introduction, as it has an index with pointers to all registered records. During this process, EHR remain with the provider and no data is stored centrally; instead, the system is decentralized. (Doupi, 2010)

#### Hong Kong (SAR), Singapore, Taiwan and Japan

In Asia, EHR projects in Singapore and Hong Kong have started, while in Taiwan at least one hospital has gone fully computerized. On an independent basis, some local hospitals and clinics in Japan have developed an EHR, and data are shared among hospitals and patients. There is no centralized government funding, support nor leadership in EHR. The EHR system in these countries is still at an early stage of development. (Arnold, 2007)

#### Australia and New Zealand

Australia's national approach to EHR was, firstly, to build the National E-Health Transition Authority (NETHA). Like Canadian Health Infoway, NETHA is a non-profit organization, but funding is a joint contribution from the national government and different states and territories in Australia (Arnold, 2007).

New Zealand is also considered to be at an advanced stage of implementation with some form of EHR. New Zealand created a unique patient identifier using the National Health Index number. There is little interoperability among health



service providers, although there are a high penetration rate and use of the National Health Index system. Pharmacists do have an interoperable system.

### United States

The EHR in the United States is not centralized, and there are privacy and security concerns associated with the use of a national centralized EHR data server model. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was passed in the US to establish rules for data protection.

Wafa (2010) argued that although the HIPPA standard created place restriction on the electronic form of information than paper format, there are still doubts about the adequacy of these standards in protecting the electronic information.

As of 2000, EHR adoption has been minimal in the US. Fewer than 10.0% of American hospitals had implemented health information technology, and about 16.0% of primary care physicians used EHRs (Johnston, Douglas, *et al.*, 2003). With a steady increase of participation, the Center for Disease Control (CDC) recently reported that the EMR adoption rate had steadily risen to 48.3% at the end of 2009 (Feingold, 2011).

Funding from the American Recovery and Reinvestment Act (ARRA) of 2009 will provide bonus payments to doctors who adopt and effectively use electronic health records. President Obama set a goal of building the infrastructure of EHR by 2015. According to Charles *et al.*, (2015), 60.0% of all nonfederal acute care hospitals adopted the basic EHR system of which 17 states have achieved 80.0% adoption of basic EHR functions.

### Canada

As of January 2009, nine years from its inception, Canada Health Infoway (CHI) had the total cumulative spending of \$2.1 billion towards developing an EHR. Canada's approach to EHR is national architecture and a blueprint established by CHI and provincial adoption as design and implementation based on specific provincial needs.

With EHR being a digital health record stored in a computer database shared by many medical service providers, there is the concern of protection against

security vulnerabilities and patient privacy in these records. Following the compliance requirement of the Canada Privacy Act (P-21), the Personal Health Information Protection Act, and the vulnerability of many information security threats on computers, it is a significant task for Canada Health Infoway to develop an infrastructure initiative to ensure that security and privacy are appropriately designed and implemented. Information security implementation and its effectiveness are most notable and successful when created at the design stage as compared to a patchwork system after the architecture are implemented (Sinnott *et al.*, 2009).

Canada Health Infoway estimates that there are about 2,000 health-care “transactions” in Canada every minute, or more than 1 billion transactions each year, including:

- 440 million laboratory tests;
- 382 million drug prescriptions;
- 332 million visits to physicians’ offices;
- 35 million diagnostic images; and
- 2.8 million in-patient hospitalizations.

(McCarter, 2009)

Over the past seven years, CHI has already marked success, completing 84 of 241 health information technology projects by the middle of the 2007-2008 fiscal years. (McCarter, 2009)

Alberta and Newfoundland & Labrador are the provinces with the highest penetration percentage and implementation of EHR. In Alberta, NetCare is the system and organization that coordinates the EHR implementation. According to the architecture of CHI, information in the EHR is classified into different roles. A physician can view more information than an administrator whose role may only be making appointments for patients.

In Newfoundland & Labrador, the Centre for Health Information provides interoperability and communication of EHR to various health practitioners and hospitals. The new Pharmacy Network implementation uses CHI architecture in the Health Information Access Layer (HIAL).

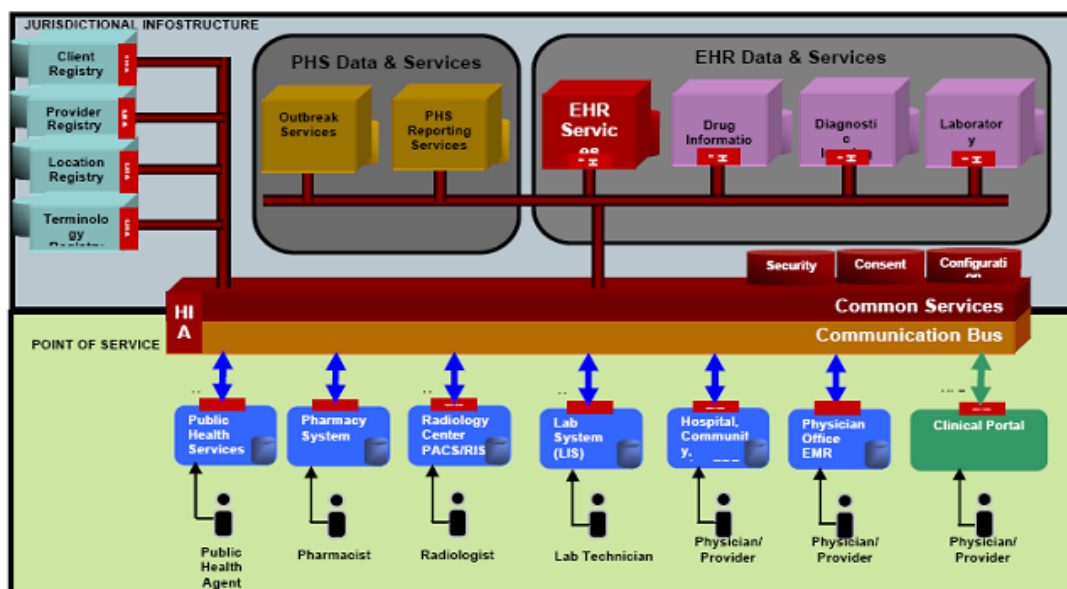


Figure 2-1: Canada Health Infoway architecture utilized in the Health Information Access Layer (HIAL)

There are four fundamental components in EHR systems that are required to provide proper functioning in Ontario. They are: (1) A secure network on which patient data can travel. (2) Applications that enable users to record, store, and retrieve patient data. (3) Patient data, such as treatment history, test results, diagnostic images, and prescribed medication, in digital form and (4) Computer terminals or access points from which users can input and retrieve patient data (McCarter, 2009).

The author observed that CHI is now using these successes as models for other provinces to follow. The lessons learned from each case are compiled in EHR "toolkits" that encourage other provinces to replicate the functioning system. As noted earlier, the implementation of the EHR is in the jurisdiction of each province. In Ontario, eHealth Ontario was established in 2008, and its mandate is to play the leading role in harnessing information technology and innovation to improve patient care, safety and access in support of the government's health strategy. There have been issues in project management within eHealth

Ontario, including over-spending and improper hiring practices of consultants on EHR projects. Such issues resulted in the removal of the CEO of eHealth Ontario in 2009 (CBC News, 2009). Since then, a new CEO has been hired, progress was made, and improved priorities set.

## 2.4 Costs and Benefits of EHR

The cost of health care in Canada has increased dramatically over the past decade. In 1997-98, the cost was 84 billion dollars and ten years later, in 2007 – 2008, the cost had more than doubled to 172 billion dollars (CHI 2009). Below is a diagram of the breakdown of health expenditure.

### Breakdown of Health Expenditure by Use of Funds, 1997–1998 and 2007–2008

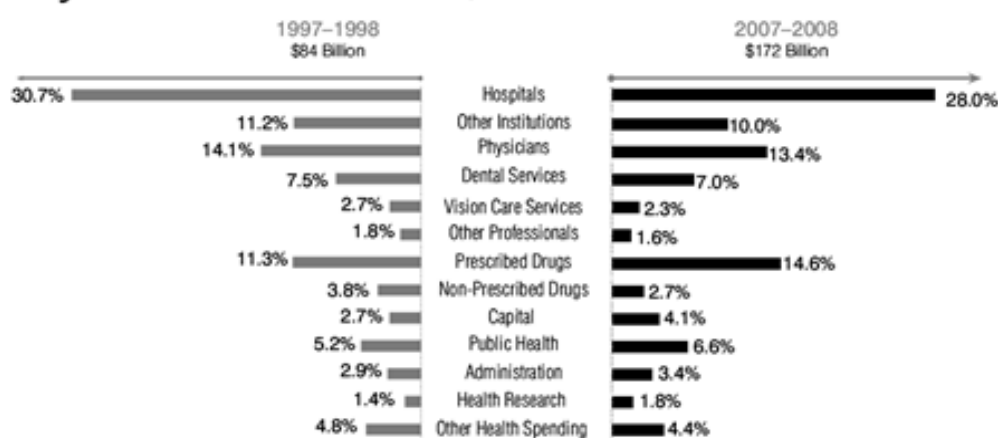


Figure 2-2: Breakdown of Health Expenditure

With this high cost, provinces like Alberta with advanced EHR implementation are running a deficit in health care expenses. Reported in CBC News in February 2010 (CBC News, 2010), Alberta's government projected a record \$4.7-billion budget shortfall and planned cuts in many departments while increasing health-care spending by 16.6%. It is a challenge for payers (governments) in many countries as healthcare expenditure has become an

increasingly larger share of GDP and government expenditures and puts considerable strain on governments to deliver services. Such increases in healthcare expenditure are particularly true in Canada where the population of senior citizens over the age of 65 from 2006 to 2020 is projected to jump from 13.0% to 18.0%. This five percent jump of senior citizens will result to an increased by 1.628 million people according to a CBC News In-depth report from Pierre Fortin, professor of economics at the Université du Québec à Montréal (Fortin, 2006).

In the same CBC News report, Fortin (2006) projected that tax revenue by the year 2020 would decrease by 4.0%, resulting in a loss of \$20 billion based on a revenue rate of \$500 billion in 2006. To add more stress to the government fiscal forecasts, for the same period of projection, health care, and social service spending will increase by 14.0%, resulting in a \$16 billion increase based on a 2006 baseline of \$112 billion. The total shortfall is projected to be 38 billion dollars (\$16 billion in health care and social services spending. As the population ages, there will be more retirees and fewer workers in Canada. There will be \$20 billion from the reduction of tax revenue, \$12 billion from increased federal payments to senior citizens, less \$10 billion from reduced education and childcare spending due to a reduced percentage of the younger age population) in 2020 (Fortin, 2006). Such a reduction of tax is not a one-time situation, and the figure may become an annual shortfall. It is in this context that provincial health spending must somehow be understood and contained.

	Total			Provincial/Territorial			Total Public Sector			Private Sector				
	Expend- iture	Exp. per Capita	Exp. as % of GDP	Expend- iture	Exp. per Capita	Exp. per Capita Growth From 2013	Expend- iture	Exp. per Capita	Exp. per Capita Growth From 2013	Exp. as % of Total	Expend- iture	Exp. per Capita	Exp. per Capita Growth From 2013	Exp. as % of Total
	\$ Billions	\$	%	\$ Billions	\$	%	\$ Billions	\$	%	%	\$ Billions	\$	%	%
<b>Canada</b>	<b>214.9</b>	<b>6,045</b>	<b>11</b>	<b>140.8</b>	<b>3,960</b>	<b>0.8</b>	<b>151.5</b>	<b>4,261</b>	<b>0.8</b>	<b>70.5</b>	<b>63.4</b>	<b>1,784</b>	<b>1.4</b>	<b>29.5</b>
<b>Ont.</b>	80.7	5,894	11.3	51.6	3,768	0.4	55	4,014	0.4	68.1	25.7	1,879	0.7	31.9

Table 2-1: Health Expenditure Summary, by Province/Territory and Canada, 2014 (CIHI 2014)

From Table 2-1 above, the figures in “Total Public Sector” included the Provincial/Territorial number, and the cost of Ontario’s total healthcare

expenditure is about 37.6% (80.7/214.9 Billions of dollars) of the provincial spending. Per capita healthcare spending in Ontario is \$5,894 - about 11.3% of provincial GDP. The significance of these costs is two-fold. For the payer (Ontario government), the implementation of EHRs system is potentially a way to control healthcare cost. For the patients, the spending of \$5,894 per capita is a benefit that is paid either by the government or from their employee health insurance benefit. Patients would like to maintain this benefit without having to pay on their own. The sharing and aggregation of their health records in electronic form could easily expose their health problem to the insurance company or the patient's employer. Such exposure may result in a reduction of their benefits.

With the implementation of EHRs, the government can obtain a better enumeration and statistics of the utilization of the healthcare system and its cost. An added benefit would be the potential reduction of redundant and costly laboratory testing and medical procedures as previous tests results are readily available from EHRs. It may also be possible to utilize the EHR information to provide decision support towards the designing of a better preventive care program before a patient's condition worsens, thus requires more health resources and increases costs.

In this context, an EHR has the potential to facilitate efficient care and to reduce duplication of medical procedures. It also has the potential to reduce adverse medical conditions that can have severe implications for patients and be costly to the payers. Paradoxically, to increase the utility of EHR, patients must be willing to share the full details of their health status and the health services they receive. However, individuals may consider their health condition be the most private information and be rightfully concerned that their private and sensitive health information will be widely shared across a digital network once it is in the EHRs system. This kind of sharing is of especially great consequence when EHR is in a digital format, making it easier for privacy vulnerabilities and mishandling of information to occur.

From a payer's point of view, EHR might also be a way to control healthcare spending. According to CHI (2004), the following expected benefits are to be achieved with EHR initiatives:

For patients:

An EHR will significantly reduce the need to provide repeatedly personal and family health history each time a patient encounters a different healthcare provider as the medical information of the patient is captured in each medical encounter and can be readily sent across a range of providers. There can be better coordination of services across providers when information is shared rapidly over an electronic network. This could also reduce duplication of diagnostic procedures. As a result, better health outcomes and reduced incidence of adverse events stemming from a lack of health information when it is needed.

For providers:

EHR implementation will improve quality and consistency of patient care through timely access to comparable data from multiple sources. Increased use of standardized and measurable information rather than from paper record with free-text only, which will allow a faster and more reliable review of health information and thus, increase user confidence. There will be reduced reliance on the verbal and anecdotal exchange of health information and more accurate and effective communication among providers. Time and resources will be reduced as duplication of effort in performing similar tests become unnecessary since results are available. CHI also suggested that there will be a higher probability of positive patient outcomes. (CHI, 2004)

## **2.5 What Are the Issues in EHR Especially in Privacy and Security Protection?**

EHR in Ontario is architected at the national level, design at a national scale with local modification and implementation at a local level. According to Stead, Kelly, & Kolodner (2005), much of the implementation of the national healthcare system will be practiced at a local level. However, EHR needs to be integrated into a national level framework with interoperability and yet accommodates with the locally distinct requirement. It becomes the fitting of many pieces of individual parts (from different provinces) software, hardware, policies, terms definitions and working together to achieve the broader goal of national EHRs system. Often, out-of-province patients may not get the full benefits of EHRs because requirements and implementation between different provinces may not be fully compatible or there may be incomplete information to the national level resulting in a weakening of interoperability. Very often, EHRs implementation across different provinces is not as congruent to the overall architecture and compatible with the national EHR system. Many existing legal frameworks of governance, policy, healthcare processes, and architecture are already in place within each province when national EHR requires the deployment and implementation the latest technologies and IT systems to support high quality and cost-effective health care system. There needs to be a balance between national control and local adaptability.

In addition to many security vulnerabilities, digital information is subject to privacy violation and exposures. The conversion of traditional healthcare records from paper to a computerized digital EHR system creates many challenges in the protection of patient privacy and security of information. The sensitive nature of the contents of medical information gives rise to hackers or internal workers seeking to exploit security vulnerabilities and capture personal information resulting in breaches of confidentiality, privacy and identity theft. According to Ravi (2008), common with any information available in the digital format, EHRs are susceptible to hacking, alteration, and, therefore, exposure of privacy, unless proper risk and change management controls are implemented.



While digital information leaves no trail on changes of information, copying, or deletion, it is difficult to ascertain the integrity of information without extensive resources protection such as encryption, policy, design, and procedures to be deployed as security protection. When information resides in computing facilities, remote access becomes a risk for different service providers, and patients may take different approaches and setups to access the data (Health Governance Report, 2007). Before granting remote access, providers and patients require the proper configuration of their secured access to the EHRs computing facilities.

Canada Health Infoway published a document titled, “The privacy and security architecture as a key component of the Electronic Health Records (EHR) Blueprint” (CHI, 2005). The blueprint ensures that the framework and vision for EHR can accommodate and respect privacy requirements across the country. Privacy rules may vary by jurisdiction, but the architecture has been designed so that the EHR can accommodate these differences. The question is how accurately and faithfully the design and architecture can be implemented in practice at the local, provincial or regional level. In addition, many security breaches are results of human errors, human circumvention, unethical access with authorization privilege and illegal compromise by hackers.

The abuse and misuse of an individual’s medical information for commercial, legal, employment, or even criminal purposes is a substantial concern in health care (McClanahan, 2008). According to Jacobson (2002), privacy violations of patient records can result in injustices such as discriminatory employment practices, invasive and embarrassing product advertising and social ostracism, for example, a patient’s positive HIV (*human immunodeficiency virus*) status being revealed.

Another risk and issue are the potentials for criminal exploitation of unprotected medical records. For example, a person suffering from a terminal illness could be targeted by criminals seeking access to his or her estate; or a married person who contracted a sexually transmitted disease could be vulnerable to blackmail and extortion. Also, medical records contain the critical ingredients of identity theft: the patient’s health insurance number, address, and date of birth

information. The ability to hack into a system that contains records of a very high percentage of people in the province is an attractive target for criminals.

The issue of different patient tolerance levels in privacy risk. There are different schools of thought regarding stakeholders' tolerance levels to risk of privacy exposure and the use of legal privacy laws to regulate privacy. Some scholars criticize such laws approach the issue from an economic perspective such as Kapushion (2004). McClanahan (2008) citing Kapushion (2004) argued that:

Using a regulatory privacy approach to protecting information privacy suffers from its generic quality and prevents the focus on consumer preferences and individual decision making that a free market approach would allow (McClanahan, 2008 pp74).

This argument is based on the idea that individual health consumers have different preferences in the degree of information privacy they desire and different valuations of what they feel health information privacy is worth. According to Hayrinen *et al.*, (2008) citing that Kapushion's view is arguing that privacy law's uniform regulation forces all health consumers to place a high value on privacy protection and feels that even an imperfect market would function better than this regulatory solution. Her premise is that each consumer (patient) has his/her level of tolerance regarding privacy risk. Another school of thought from legal scholars such as Solove (2004), expresses skepticism that the market alone is up to the challenge of protecting medical information privacy. This opposing argument asserts that market-based controls are powerless to prevent the abuse of individuals' private records by third parties. Another reason is that when commercial entities use their own privacy policies (which are contractual approaches), consumers are often left with no bargaining leverage to negotiate or enforce compliance with the policy. Solove (2004) further argues that unlike common goods and services, market forces alone cannot effectively curtail violations of the privacy of individuals' electronic information because the online environment allows these offending bureaucracies' and commercial entities' violations to occur, often without the victims being aware that these offences have happened. It is impossible for consumers to bring economic

pressure to bear on the situation when they do not realize they have been wronged (McClanahan, 2008).

In the USA, privacy concerns in health care apply to both paper and electronic records. Lake Research Partners and the American Viewpoint, (2006), found that roughly 150 people (from doctors and nurses to technicians and billing clerks) have access to at least part of a patient's records during hospitalization. This research also indicates that up to 600,000 payers, providers and other entities that handle providers' billing data have some access to the patient's private information. Such large number of the eligible persons seeing the private information of the patient could lead to vulnerabilities and privacy breaches.

In the same report, Lake Research Partners and America Viewpoint, (2006) has released the result of a national level survey in the USA. Of the 1003 patients who responded to the survey, 80 percent reported being very concerned about identity theft or fraud; 77 percent were very concerned about the use of their medical information for marketing purposes; 56 percent worried that employers would access their health information, and 55 percent were concerned about insurers. The survey uses random digit dialing (RDD) probability sampling. The margin of sampling error for the survey is 3.1%.

Americans have expressed strong privacy concerns including concern that their information may be used for purposes other than their own healthcare. This research seeks to examine if a similar pattern of patient concerns exists in Canada and to interpret them in the context of an emerging EHR information system. Such reviews may expose an early warning of Canadian concerns that can be dealt with while the EHR is still in the implementation stage.

A study from the University of Otago (Chhanabhai, 2007), New Zealand was conducted to determine the perceptions held by patients in New Zealand with regards to their concern of security of an EHR. A significant finding from a sample size of 300 participants, is that there were concerns about privacy, security, and confidentiality of their health medical records. The survey was done in four major cities in Auckland, Wellington, Christchurch, and Dunedin.

The findings were considered valid and meaningful based on the sample size of the study.

However, there is little concern of security between the difference in using health record in the paper form or the electronic form (Chhanabhai, 2007). These findings align with similar results found in many US patient surveys. It is also important to note that health care concerns exist regardless of format (electronic/paper). However, an EHR may have more concerns. At a minimum, it suggests that there are concerns about information sharing and that these are likely to play a role in any attempt to implement an EHR.

Similar incidents of EHR security breaches have been reported in other EHR systems such as the UK. In Oct 2012, The Telegraph (2012) said that there were sixteen major incidents and that over 1.7 million patient records were lost within the year. This included a single incident of 1.6 million patient records stored on a CD was lost during an office move. In 2013, the NHS lost over 3,000 patients records in their auctioning of a second-hand computer in eBay. (BBC News, 2013)

In Ontario, Canada, patients have justified concerns that their private and sensitive information is being compromised. Such compromise includes the frequent mishandling and the loss of private patient information. For example, in Canada, the Office of the Information and Privacy Commissioner of Ontario has dealt with the failure of proper handling of private information of patients:

- (1) The Durham Regional Health Authority reported that a nurse lost a USB key containing health information of almost 84,000 patients who attended H1N1 flu vaccination clinics (Cavoukian, 2010).
- (2) Without obtaining the patient's consent, a newspaper published the photograph of a patient in a hospital while he is a patient in a hospital. (IPC, Oct 2005a).
- (3) A hospital's fundraising foundation received personal health information about a former patient without the individual's consent (IPC, 2005b).

- (4) Patient records ended up strewn across Toronto streets to help a film company make the site look like New York City after 9/11 (IPC, 2005c).
- (5) A service provider refused to correct a patient file that contains the discussion that the patient claimed it had never taken place (IPC, 2005d). The issue is who owns the health information and the accuracy and correction procedure of health information.

In 2007, Canada Health Infoway (CHI) and The Office of the Privacy Commission of Canada sponsored a survey conducted by Ekos Research Associates entitled “Electronic Health Information and Privacy Survey: What Canadians Think—2007.” Researchers contacted 2,469 Canadians aged sixteen and older in June and July for over-the-phone interviews of about twenty minutes in length. There were 17 percent respondents considered information about them held by the healthcare system as not very safe and secure. 40 percent thought it was “moderately safe and secure” and 39 percent thought it was “safe and secure” (Ekos, 2007). The survey noted that over the past four years, there had been an erosion of trust by Canadians in healthcare workers and organizations over whether they could keep their information safe and secure.

In April 2012, CHI conducted a second privacy survey nationally across Canada. There were 2,509 Canadians aged 16 years and older surveyed using mixed methodology: telephone and online. There were 1,300 participants in the telephone survey and 1,209 online.

The CHI survey results are positively related to some of our hypothesis. The survey (Ipsos Reid, 2012) result showed that eight percent of respondents oppose to EHR. They are concerns about the safety of health information and privacy or confidentiality of their EHR information. It also found that 85 percent of respondents believe people withhold health-related information from their doctor. Also, concerns about unauthorized access and distrust of the computer systems are evidence than their last survey. Thirty-eight percent of respondents indicated that they are only “somewhat” supportive of the EHR. It appears that some respondents are skeptical of the success and benefits of EHR and therefore taking the “wait and see” attitude pending further implementation of EHR system.

## **2.6 The literature on Assessment Model of Privacy and EHR**

Smith, Milberg, and Burke (1996) developed and validated a 15-item survey instrument (CFIP – Concerns for Information Privacy) that measure different dimensions of an individual's concerns about information privacy.

This CFIP model has laid the foundation for standard measurement of concerns for information privacy by using these six dimensions. Their study was cited in 377 other scholarly journals, including subsequent work done by Stewart & Segars (2002) in which they confirmed the validity of Smith, Milberg and Burke's CFIP instrument in that the dimensions described comprise a valid framework.

Stewart & Segars (2002) have further expanded upon the sample from Smith, Milberg & Burke, (1996) with studies using employees of financial institutes and professional members to a much broader cross-section of the human population of consumers. They have integrated the CFIP model and the elaboration likelihood model (ELM) to examine attitude change and the likelihood of opt-in an EHR system. Angst & Agarwal (2009) investigate the question: "Can individuals be persuaded to change their attitudes and opting-in behavioral intentions toward EHRs, and allow their medical information to be digitized even in the presence of significant privacy concerns?" The result showed that "even when people have high concerns for privacy, their attitudes can be positively altered with appropriate message framing," (Angst & Arwal, 2009).

## 2.7 Gaps in the Literature

Based on the literature reviewed, the following gaps have been identified:

- (1) There have been very few studies on patients' sensitivity in releasing private information to service providers. Angst & Agarwal (2009) found that patients' adoption of EHR is influenced by the use of EHR and their concern for information privacy (CFIP). They also found the service provider could positively influence that patient's adoption rate in how they frame the message to the patient. This research study centers on the hypothesis that patients are more likely to opt-in to provide private information pending the severity of their illness. There is also an opportunity to examine if there is a patient who will not provide their private information even if their disease worsens, as they do not trust the EHR system.
- (2) In this research study, there is an opportunity to expand Smith, Milberg and Burke's CFIP framework from heterogeneous groups of executives, consumers, judges, and students to a homogeneous group of patients using an EHR system. This can also be a lateral expansion from Stewart & Segars' study of consumers to the subscriber. This gap in literature allows for contribution to the assessment of patient risk attitudes toward the private information stored in EHR. Such information may be considered by patients to be very sensitive and private in nature. There is potential for serious adverse events if private information is withheld by patients.
- (3) The literature search revealed that there are very few papers that discuss the needs of the providers regarding their information needs to provide quality health care. The author intends to research this area to fill the gap in the literature.
- (4) Angst & Agarwal (2009) indicated that they had used a single item measure of the likelihood of adoption for which they are unable to assess reliability. The single item measure used is the framing of health message in a positive and neutral argument frame upon which patient made their opt-in or opt-out option to provide extra information to EHR. According to Wanous *et al.* (1997), single item measure is only adequate when the message is

unambiguous, and it can be interpreted. In our opinion, this kind of single measure neglects the patient's emotions during their sickness and other factors such as optimism and their relationship with the service provider. When dealing with psychological constructs, such as multi-criteria decision-making activities or the risk attitude of privacy protection vs. quality of medical care with full disclosure, single item measures are discouraged because they yield low reliability. For this reason, Angst & Agarwal suggested that future research should employ multi-item scales. This gap in the literature allows the author's positioning of multi-item scale using, in addition to a single item measure using survey questions, the use of scenario-based multi-criteria decision making (conjoint analysis) questions in part 2 of the survey allows the examination of patient decisions towards severity of their medical condition.

- (5) Most of the studies are conducted in the US. There has been very little work done in Canada or specifically in Ontario. A study of patient privacy and security attitudes towards EHR systems in Ontario allows for an empirically confirmatory study to compare results of the US study.
- (6) There have been many kinds of studies published in protecting private information while distributing in a network such as using encryption techniques and service-oriented architecture design. One paper specifically applied to healthcare is Siegenthaler & Birman (2009) which fits the EHRs data environment of information being transmitted over distributed databases located in provider's environment. Like most of the published literature, the discussions are an attempt to solve the protection by engineering technical procedures and solutions such as utilizing distributed query engines, and bootstrapping the system when identity is confirmed (Siegenthaler & Birman, 2009). Very little has been written in the examination of human elements and human attitude towards the sharing of the private and sensitive personal information over a distributed communication network. This study attempt to understand the human side of the privacy. The technology controls and the hardware or software application in security implementation is not the scope of this study.



## 2.8 Research Questions

From the literature review, there is evidence that stakeholders, especially patients, have concerns about the privacy and security vulnerabilities of EHRs. Patients from the USA have exhibited various behaviors to take responsibility for protecting their private information. The focus of meaningful research is to investigate and measure patients' willingness to provide and share private information with providers and to contrast this with the information needs of the providers and payers. Since the EHRs system in Ontario is not yet fully implemented, this research is particularly important because the utility of the actual EHRs could be greatly compromised if patients' privacy issues are not adequately dealt with at the design phase.

As in studies found in the USA reported by Irwin (2018), patient withholding of private information creates a paradoxical constraint to both parties: patients and providers. This is especially so for service providers who require this information to provide efficient and cost-effective medical care. There exist many adverse events resulting in providers not having access to crucial information at a time when a clinical decision is being made.

Based on the literature review, the critical question for this research study can be formulated as followed:

“What are the perceived risks surrounding the sharing of private and sensitive health and personal information with health care providers and potentially having the information distributed across the health system?”

The primary research question gives rise to some sub-questions that need to be addressed. They are described below.

### **2.8.1 Research Sub-questions**

The following sub-questions are developed:

- (1) What level and the types of perceived privacy risks (e.g., excessive collection of data, unauthorized secondary use of data, improper access of data and errors of data) are of privacy concern in EHR implementation?
- (2) How willing are patients to give out sensitive and private information to service providers when their medical condition is deteriorated?
- (3) Do patients think that providers can keep their data secure and private?
- (4) Is patient's gender a factor influencing the level of privacy concerns?
- (5) Is patient's age group or career stage a factor influencing the level of privacy concerns?
- (6) What level of information access and control do patients want to have over their private data in an EHR system?
- (7) What are providers concerns on EHR systems?
- (8) Do providers have privacy concerns in EHRs as they also placed their personally identifiable information, diagnosis, and notes in the EHR?
- (9) What are the challenges and concerns of payers in their implementation of EHR?

### **2.9 Concepts of Countermeasures**

Jenson W (2000 p.1667) argued: "Countermeasures typically include any action, device, procedure, technique, or another measure that reduces the vulnerability of or threat to a system."

As introduced in section 1.3.1 concept 5, the author is interested in finding out the extent of countermeasures used by patients in their reduction of the risk and impacts of privacy exposure. Countermeasure is often used in information system security or military system security. Very few studies on patient behavior and actions are framed and analyzed with the concept of

countermeasure. Many papers study countermeasure in the context of information systems (Furnell, *et al.*, 2002; D'Arcy & Hovav, 2007) but few studies the human behavior (patient) in their action to countermeasure the risk and impact of their privacy exposure. Yeh & Change (2007) argued that the information system in the industry, such as a financial institution, with higher-level computerization and a higher-level of perceived of security threat, should deploy the higher level of countermeasures than that of the lower level of computerization system used in the manufacturing industry.

By extending this argument, the author suggests that the benefits of EHR are based on high-level computerization of database, network transportation and the computer storage and retrieval of the precise and correct records in the Electronic Health Records system. From a patient's perspective, the level of threat in the breach of their private and sensitive health information is high as evidenced in the many violations of privacy protection as described in section 2.5. Given such high-level of computerization in EHR system and the high-level of threat and impact to the patient, extending to Yan & Chang's (2007) argument to human behavior, the actions to countermeasure from patients could be high and severe.

## **2.10 Validity and Relevancy of This Literature Review**

According to Brown (2006), there are five criteria for the evaluation of the validity of literature review: purpose, scope, authority, audience, and format. Accordingly, each of these criteria has been taken into account and appropriately addressed during the process of the literature review in this research study. The items on purpose, scope, and authority are discussed below.

Similarly, Levy and Ellis (2006) suggested that a literature review should accomplish the following points:

(1) Allow the researcher to understand the existing body of knowledge where excess research exists and where new research is needed. From the literature review described in this chapter, the author attained the purpose of finding out what has been done (excess research) in the body of knowledge domain in EHR. These included existing studies in the different approach to EHR designs worldwide from the top- down approach to bottom-up approach. The costs to design, build and implement and maintenance of the EHR initiatives and benefits to patients, providers and government such as help maintain a healthy citizenship and labor markets, public health implementation, the establishment of an extensive medical database. Conversely, the gaps and areas of new research such as privacy and patient's concerns, human behavior of countermeasures, the patient's demographic information such as gender, age, and the career stages in their work life. Very few studies have touched on these parameters in the topics of privacy, the efficacy of EHR.

(2) Providing a solid theoretical foundation for the proposed research. Through the process of literature review, the CFIP model has been found to be a proper and comprehensive theoretical foundation for this research study. The scope to include the 3Ps (patients, providers, and payers) is grounded in the use of a research design increasing the validity and reliability of the findings.

(3) Substantiating the presence of the research problem in this literature review, scholarly research discusses many issues: with EHR implementation of federal specifications and local implementation (Stead *et al.*, 2005). There are the vulnerability issues of digital information (Ravi, 2008), and surveys from California HealthCare Foundation (1999) showed how patient have taken evasive and countermeasure actions to protect their own privacy as they perceived the threat of privacy breaches.

(4) Justifying the proposed study as one that contributes some new knowledge. The literature review helps in solidifying a research topic in social attitude and humanistic actions of patient's need for privacy protection and the necessity of efficacy from the government payers. The literature review has shown many studies have been done reviewing the scope of technology in EHR design, implementation and it associated information systems.

(5) Framing sound research methodologies, approach, goals, and research questions for the proposed study. The lack of holistic approach in investigating the patient's concern prompted the use of a mixed method of quantitative and qualitative approaches to obtain research data to increase the validity and reliability of finding. The method to enhance validity and reliability of findings is by using a triangulation design and Delphi techniques. The research instruments of using survey, focus group, and key informant interviews are a result of not finding many holistic approaches in the literature review.

To adequately address the research topic in privacy, it is noted that in addition to the scholarly discussions and academic literature used in this thesis, many of the privacy discussions are from law journals to survey the legal definition of responsibilities and infringements of privacy. Service providers practice healthcare in which the ethics and appropriate practice of privacy are well defined by their professional bodies. It is essential that the literature on the regulation and professional standards are explored. From a patient's point of view, incidents of breaches of privacy are often learned from the media news reports. In this regard, reputable and evidence-based news reports are surveyed as part of the literature review.

As discussed, privacy invokes the proper use of EHRs when implemented with the standards and regulations defined by professional health and legal practice. Therefore, this literature review includes the domains from legislative laws, professional ethics and practice standards as well as cases of privacy violation. Careful screening of the creditability and authority of the source of literature is done to avoid marketing or politically charged literature.

## **2.11 Chapter Summary**

This chapter has established a review of existing knowledge relating to patient privacy in EHRs. The review highlighted many EHRs initiatives worldwide, the motives of payer's initiative of EHRs, the issues that may give rise to patient privacy concerns. While establishing the reasons and validity of privacy concerns of patients in EHR, an established research framework, namely Concerns For Information Privacy (CFIP) developed by Smith, Milberg and Burke (1996) in accessing privacy, is identified and discussed. The validity of the CFIP framework has been confirmed and expanded subsequently by other researchers through new research studies. By defining the research question and sub-questions, it allows the author to decide a research methodology and a research design that can provide an overall strategy integrating the different instruments and approach to form a coherent and a relevant study of the research questions.

## **Chapter 3 Research Methodology and Design**

### **3.1 Introduction**

This chapter begins with a discussion of beliefs leading to knowledge and the author's philosophical perspective as a critical realist that guide the research methodology and design. Building upon the research questions from Chapter Two, the author has constructed a framework and a set of hypotheses that provide a discussion of the research approach, design, and protocols. The methodology used to gather and analyze data is described. The details of the plan for recruitment of the 3Ps (Patient, Provider, and Payer) in this study are presented. Also, guidelines with questions for the patient survey, focus groups, and key informant interviews are included. This chapter ends with a description of some of the challenges encountered and mitigation strategies devised while conducting the selected methodology.

### **3.2 Propositional Knowledge in This Research**

Propositional knowledge is the type of knowledge that by its very nature is expressed in declarative sentences or indicative propositions. (Fantl, 2016; Gemma, 2014). It is an important and a common concept that "belief" requires reasoning to become justified knowledge. This research study seeks justified knowledge to add to the current body of knowledge in the domain of Electronic Health Records. The propositional knowledge resulted from the findings, and the interpretation of patient attitudes toward privacy in EHR can be explicated if one understands the context of patient's experience and the knowledge in the EHR environment. It is appropriate to obtain information through survey and

scenarios questions to assess the reality perceived by patients. Patients' decisions for countermeasure and antithesis to the EHR environment are depended on their belief for which it becomes a foundation in knowledge. To this end, it is important for us to appreciate what knowledge is. According to Craig (1998, p.4367), "knowledge is knowing of true beliefs that are based on sufficiently good reasons". A true belief in this sense is a justified belief. "Plato came up with the standard definition of knowledge: what qualifies a true belief as knowledge is ... justification" (MBSW 2006 p.12).

In formal terms, an agent S knows that a proposition P is true if and only if:

- (a). P is true
- (b). S believes that P is true, and
- (c). S is justified in believing that P is true

For example, in this research study,

1. P is a proposition that "It is possible for a custodian to lose their EHR records under their protection in a large quantity at one time."
2. Patient S believes that proposition P is true in the context that the proposition P can happen
3. Patient S is able to provide evidence of incidents that happened to match the proposition P. Examples of such incidents include those incidents described in Section 2.5 above: (1) A nurse lost 84,000 EHR data in Durham region. (2) Patient records ended up on across Toronto streets to help a film company make the site look like New York City after 9/11. (3) A doctor lost a computer hard disk containing 3,300 patients' electronic health record despite an early order forbidden the removal of EHR from the hospital where the doctor works.

Based on the above information, patients S in Ontario have justified the belief that provider who acts as custodian indeed, have loss EHRs in a large quantity at one time (i.e. Proposition P). Therefore, patient S has a justified true belief and according, knowledge of P. There are concerns about the loss of EHR information from medical care providers. Such loss could lead to possible exposure of patient's sensitive and private medical information. In Chapter



Seven, the author will discuss the newly found justified belief from this research study using triangulation design to assess the preliminary findings of this research by the 3Ps to identify justified true belief into knowledge.

There are different philosophical perspectives on what qualifies a belief to become knowledge. Foundationalists claim that knowledge came about from a sequence of reasoning that some beliefs ultimately rest on a fundamental belief that requires no justification (Craig, 1998 p.4367; MBSW p.21). In contrast, coherentists argue that there are no foundational reasons, but rather a web of beliefs that mutually support each other (Craig, 1998 p.4367; MBSW p.21; Bernecker and Dretske, 2007 p.128). Foundationalist theory is criticized because of its premise that belief can have infinite regress with one belief built upon another. Meanwhile, the drawback of the coherentist theory is that belief can form a circular path. Also, there is a third theory of knowledge constructed by contextualists.

“The contextualist answer [to a question] is we all understand that what counts as knowledge is always relative to a context of justification” (MBSW 2006, p.28). This research study is within the realm of a contextualist in that knowledge related to EHR that obtained from surveys, scenario questions, discussion group, and key informant interviews are explicated under the context of justification. As discussed in the above paragraphs, the author seeks to understand the patient's concern about privacy under the context of patient's true belief and their formed knowledge in the EHR environment

How does one know that belief is true? According to the view of a contextualist, one option is to evaluate the certainty of the belief. Belief requires some form of justification to ascertain that it is true in order to become knowledge. The quantity survey of the questionnaire, the assessment of patients' perceived action given a scenario is to understand the patients' belief that form knowledge and subsequently formed their attitude. The conducting of focus group discussions with health service providers and the key informant interviews with many government officials (providing the perspective of payers) is to attain knowledge and belief from these two important stakeholders group

of the EHR systems that might be able to explain the issue in privacy and the resulting attitudes of the patients.

### **3.3 Philosophical Position of this Research**

In this study, while a contextualist approach in selecting an appropriate framework to obtain data, the author assumes a position as a critical realist in order to make sense of the data obtained and interpret observations collected. Relevant validity is grounded in the discussion chapter (Chapter Seven) from a contextualist perspective. The author attempts to highlight the characteristics of discussion and understand the knowledge relative to a context of justification. It is essential to understand that some of the philosophical terms related to this research.

Ontology refers to a philosophical concept of the study of nature of being and the reality of the external world. Positivism refers to the view that valid knowledge (truth) exists only in scientific knowledge. Verified data received from the senses is known as empirical evidence (Macionis and Gerber, 2010). A positivist position in social science research such as the attitude of patient concerns about privacy in Electronic Health Records will suggest that the social world operates similarly to the natural and physical world. The author's focus is on critical realism in the attempt to explain the reality of patient's attitude in a social world.

### 3.4 Critical Realism

In this research study, the author took a philosophical view of knowledge from the perspective of critical realism (CR) to interpret data, attitudes, beliefs, and experiences described from the 3Ps. The author accepted that knowledge about patients' attitudes of privacy concerns to the external EHR system is perceived through their human minds. The reality of the security protection of privacy information in the EHR system may be modulated by how a patient's perception of privacy risk differs from that of the system. Patient perceptions of privacy risks of EHR systems may become a reality in the mind of the patient.

Experience allows a patient to form perceptions. Perception is the fundamental form of forming opinion and belief. It is this belief that motivates and drives the behavior of the patient. At times, this perception may not be the entire truth of the situation. For example, the payers who are in charge of the design and implementation of EHR does not conduct proper and adequate education to patients such as the disclosure of objectives and level of implementation of privacy and security protection. Without this important distribution of knowledge from the payer, patients are left to form their own knowledge on their concern for privacy in the EHR system. Concurrently during this period of forming their opinion towards the EHR, patients often hear from the media about the many incidents of hacking and mishandling of private information in the electronic healthcare records.

The following could be a scenario where patient underestimated and undervalued the ability of the EHR system for the protection of patient privacy. Payers may have inadequately educated and provide the necessary assurance to patients the level of privacy protection in the EHR system. The patient is then left alone to receive information about the story of the privacy breach and negative publicity from media, that led to patient's lack of confidence in the EHR system. It is this perception of EHR becomes the perceived reality of the patient. Such reality may be different from the actual reality of the capability of the EHR system. A patient's perceived reality in the social world through information from media and social interactions with other patients could lead to

a subsequent countermeasure behavior that becomes less relevant to the actual reality of the EHR system.

Critical realists recognize the reality of the natural world as well as the events and discourses of the social world (Wikgren, 2014 p.14). According to this view, one will only be able to understand and, therefore, change the social world if one identifies the structures at work that generate those events and discourses (Bhaskar, 1989).

The critical realism theory suggested that there is a reality exists independently of its human conception. Critical realists believe that there are unobservable events that cause the observable ones; hence, the social world can be understood only if people understand the structures that generate such unobservable events (Larsen *et al.*, 2015). The author hypothesized that patients' attitudes towards the privacy concerns in EHR, via the observable events from social world and their interaction with the provider, could be a cause (or a result) by the payers and providers actions and designs. Such action and designs are related to the structure of EHR systems (including choices made by the EHR implementation team) that are not readily observable by the patient.

Following our position of critical realism in this research, the author has carefully selected a research methodology employing a mixed-method approach using quantitative and qualitative methods. This research uses a triangulation research design on data and analysis, with time, space, and persons. Instruments to collect data surveys, focus group discussions and key informant interviews with each type of data collected over different time, different space and with different individual or group of people. By doing so, the author attempts to uncover unobservable events and design factors in EHR that could constitute (explain) the observable phenomenon of the patients.

It is to this end that this research uses a quantitative survey instrument to validate that patients have a real concern for privacy and qualitative instruments (scenarios in surveys, focus group discussions, key informant interviews) to understand outcomes of patients' decisions and choice of action arising from their attitude towards EHRs. Key Informant Interviews are used to uncover some of the unobservable structures of EHR systems, which in turn influence

the level of patient privacy concerns. Such unobservable matter could be the discussion of belief and perceptions of the designer during the interview. Such perception and belief of these developers of EHR system, cannot be observed or obtained from the available document by the patient. Another example is after our focus group discussion with service providers, some of them have their own concerns about their privacy protection regarding their medical notes and opinion left on the EHR system. The countermeasure taken up by the provider may not be observable by patients.

### **3.5 Research Methods**

The author approaches this research study by using a mixed-method with pre-designed questions and scenarios for quantitative and qualitative data collection. Patient attitudes are evaluated using scenario survey composed of categorical data design. Focus group discussions and key informant interviews were conducted using qualitative methods. Flexibility is by design, as part of the qualitative data collection, to allow for the exploration of any specific topic of interest that a participant would like to expand on during the focus group discussions or key informant interviews.

The common and well-known approach to mixed-method is the triangulation design (Creswell *et al.*, 2003). The purpose of this design is “to obtain different but complementary data on the same topic” (Morse, 1991, p. 122) and to better understand the research problem. In most cases, mixed methods require the quantitative and qualitative parts of the research to be executed in the same phase and with equal weighting.

One of the reasons for this mixed research method is to enable the capturing of data for analysis beyond patients’ attitudes. It facilitates an understanding in some of the unobservable events in the EHR systems (Payer, Providers and the

EHR info-structure), which consequently, provide knowledge on privacy and efficacy of the EHR system in the Greater Toronto Area of Ontario.

As discussed in Section 2.10, to increase the validity and reliability of findings, this research uses a triangulation design and Delphi techniques. The research methodology of using: mixed quantitative and qualitative method; the Triangulation design; the Delphi technique; the research models of 3Ps and the theoretical framework of each of the 3Ps provides a holistic approach to a social study of human perception and behavior in EHR. This holistic approach will fulfill the gaps uncovered in the literature review described in section 2.6.

(a) The research method and scope of studying centered on the human perceptions and action side of the 3Ps in their privacy concerns about EHR. This scope is in contrast to the gap when most of the literature is focused on the machine side of the EHR information system and the technical solutions. A holistic approach by triangulating the evidence and findings with data from the service provider and most literature are on the topic of patient care and disease curing. Very few health informatics papers focus on privacy in Electronic Health Records.

(b) Few articles on the social aspects of patient's attitude towards EHR and how the patients are protecting themselves using countermeasure to reduce the risk and impact of privacy exposure. Some social surveys have been done, but none considers the provider and the payer side.

(c) In the knowledge domain in EHR research, there is a gap in the existing literature which lacks the use of a multi-subjects and holistic approach to obtaining data and findings for privacy concerns in EHR. This research uses 3Ps, triangulation analysis and validity of findings from three different data-sets. This is in contrast to Angst & Agarwal (2009) which is expanded in the point (f) below.

(d) The service providers who are both users (using payer's design) and a practitioner (deploying EHR to address the medical conditions of patients) could also have concerns about their privacy protections. There is a gap in

literature studying the privacy concerns of service providers and countermeasure that may be initiated by providers.

(e) There is an opportunity to expand Smith, Milberg and Burke's CFIP framework from heterogeneous groups of executives, consumers, judges, and students to a homogeneous group of patients using an EHR system.

(f) Angst & Agarwal (2009) indicated that they had used a single item measure of the likelihood of adoption for which they are unable to assess reliability. The single item measure used is the framing of health message in a positive and neutral argument frame upon which patient made their opt-in or opt-out option to provide extra information to an EHR

### **3.6 Research Models**

The following two models will provide a contextualist approach in guiding this research project.

#### **3.6.1 Using the 3Ps models for Three Different Stakeholders Group**

By using a contextualist domain, the scope of the study is framed with three stakeholders (the 3Ps). By utilizing a triangulation design which included the surveying of Patient group, conducting a focus group discussion with Providers and interviewing Payers to give a comprehensive picture composed of data description of reality. This establishes an epistemological nature of knowledge that derived from various views and become justified true belief.

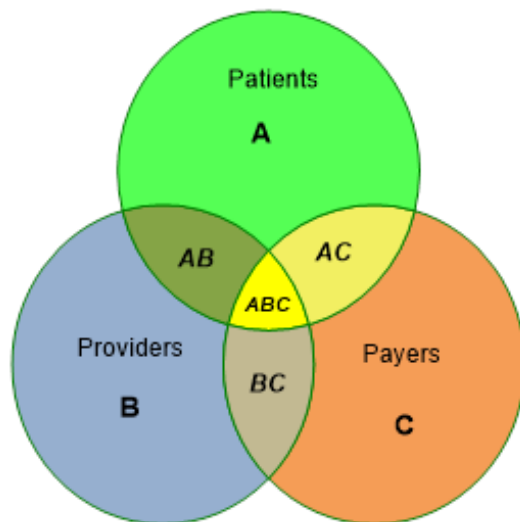


Figure 3-1: Logical view of 3P relationship in the sharing and control of information.

The following figure gives a logical presentation of the interactive information control and willingness of information sharing among the 3Ps.

A = Patients' most private and sensitive information which is not shared with providers nor payers.

AB = Patient information shared only with the provider and may be a trade-off for quality health care.

AC = Patient is willing to provide information in exchange for benefits. For example, financial benefits from the reduction of duplicated tests.

B = Provider information that is confidential and not for disclosure, such as doctors' confidential diagnosis notes and observations.

BC = Provider information shared with the payer. For example, billing information to the Ontario Health Insurance Plan (OHIP) after providing services to patients enrolled in OHIP.

C = Confidential information not shared by the payer, such as strategic plans, cost variants and cost controls that are not for sharing.

AC = Information that payers are willing to share with patients such as billing information.



ABC = Information that the 3Ps must share for the EHR system to be functional.

Depending on the findings, the Venn diagram could also show a complicated relationship between the 3Ps and the EHR system and that they may be interlocked together in a complex configuration.

### **3.6.2 Concerns For Information Privacy (CFIP) Framework**

The sharing of patients' sensitive information in an EHR framework gives rise to concerns of privacy violation. It is difficult to assess the individual value towards their risk attitude of privacy violation. Smith, Milberg, and Burke (1996) developed and validated a 15-item survey instrument (CFIP – Concerns for Information Privacy) that measures the six dimensions of an individual's concerns about information privacy. These six dimensions are:

1. An extensive collection of data --- the concern that extensive amounts of personally identifiable data are being collected and stored in a database.
2. Unauthorized secondary use of data --- the concern that information is collected from individuals for one purpose but is used for another secondary purpose (whether internally or externally to the collecting organization) without authorization from the individuals. Improper access refers to concerns that data about individuals is readily available to people not properly authorized to view or work with the data.
3. Improper access to data --- the concern that data about individuals are readily available to people not authorized to view or work with that data.
4. Errors in data --- the concern that protection against deliberate and accidental errors in personal data is inadequate.

5. Reduced judgment --- the concern that automation of decision-making processes may be excessive and those mechanisms for decoupling from automated decision processes may be inadequate.
6. Combining data --- the concern that personal data in disparate databases may be combined into more extensive databases, thus creating a “mosaic effect.” This means that a combination of seemingly harmless bits of data can create a privacy breach when combined at a more substantial databases level.

(Smith, Milberg, & Burke, 1996 p172).

In this research study, the author adopts the first four dimensions described above in the patient attitude survey. From a contextual point of view in the defining the scope and framework, the first four domains are easily understood by patients than that of dimension five and six. Also, as the EHR system is still not fully implemented in Ontario, this would have a less impact from privacy breach in dimensions five and six above. It is noted that some part of dimension six will not be in the patient survey but will be in the providers’ focus group discussion and payers key informant interviews as a mean to uncover events that may be unobservable by the patients.

### **3.7 Theoretical Framework and Hypothesis**

An underlying question to the patient’s attitude in this research is whether there are any patterns of utility behavior at work. That is, whether there are any “trade-off” decisions at work between patients and service providers. Such a trade-off could influence the decisions of the patients in their trading of privacy protection in return for a perceived better medical treatment or quality of their health record information in case of future medical emergencies.

### 3.7.1 Patients

Two frameworks were created for quantitative and qualitative (mixed-method) research.

#### Quantitative Survey Framework

The first part of the patient survey listed in Appendix A is to confirm patient concerns about information privacy as per the CFIP model (Smith *et al.*, 1996).

The construct of shown in the framework suggested that patient's willingness to share private information is dependent on their established attitude towards EHR. Their attitude is intervened by the level of severity in their privacy concerns under the four CFIP domains chosen for this study. The author suggests that a patient's attitude towards risk; trust of the EHR system and relationship to the service provider will moderate the patient's willingness to provide private information. These moderation factors will be interpreted using the patient's age and gender data in the subsequent analysis.

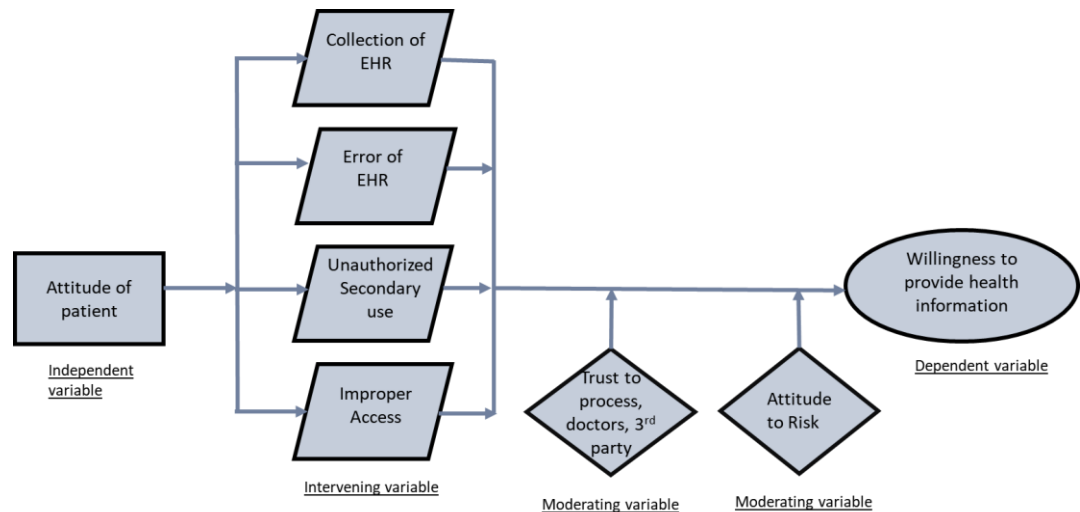


Figure 3-2: Quantitative survey framework for patients

### Qualitative: Scenario-based Survey Framework

The second part of the same patient survey in Appendix A measures the decisions and countermeasure actions made by patients based on the various hypothetical scenarios presented to them.

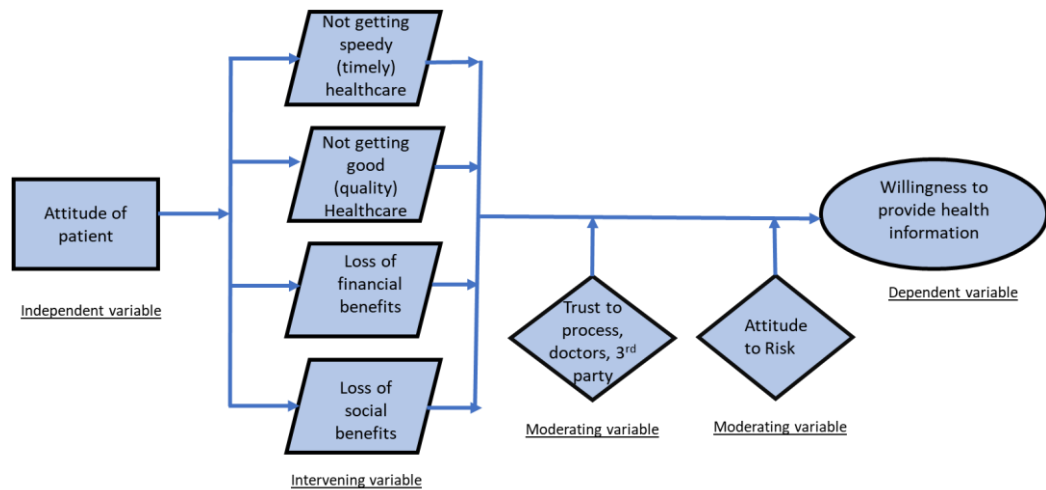


Figure 3-3: Qualitative survey framework for patients.

Different patients have different attitudes (different comfort levels) towards the disclosure of their private information. Patients, in general, will disclose their private information progressively under the progression of the severity of their medical conditions. Providers can deliver increased service level improvements when EHR information is more comprehensive because of patient's willingness to share private and sensitive information relevant to their illness. Insufficient or no input from patients in the design and development of EHR system will decrease the cooperation rate from patients in entrusting their private information to the EHR system.

Surveys are an efficient and useful tool for collecting data. It is time-efficient in obtaining a significant amount of data and effective coverage of a large sample when compared to qualitative interviewing or a limited case-study methodology for this research topic. A copy of the survey questionnaires can be found in Appendix A.

### 3.7.2 Service Providers

#### Focus Group Discussion Framework

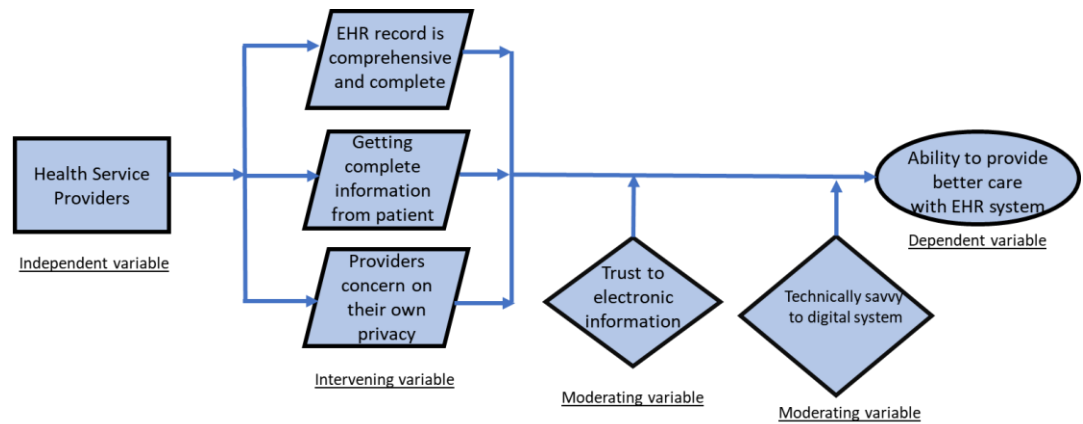


Figure 3-4: Focus group discussion framework for health service providers.

An increase in the comprehensiveness of data within the EHR systems will increase the service provider's ability to provide better patient care. An improvement in the accuracy of the data within the EHR systems will enhance the ability of the service provider for better care of patients. An increase in the completeness of data within the EHR systems will increase the service provider's capacity for better care of patients. Also, an increase in the service providers concerns with the own privacy in the EHR system will decrease their or other provider's ability to provide better patient care. Finally, if service providers are more familiar with digital computer systems as well as having a high level of trust with the EHR system, they will be able to provide better quality patient care.

### 3.7.3 Payers

#### Key Informant Interview Framework

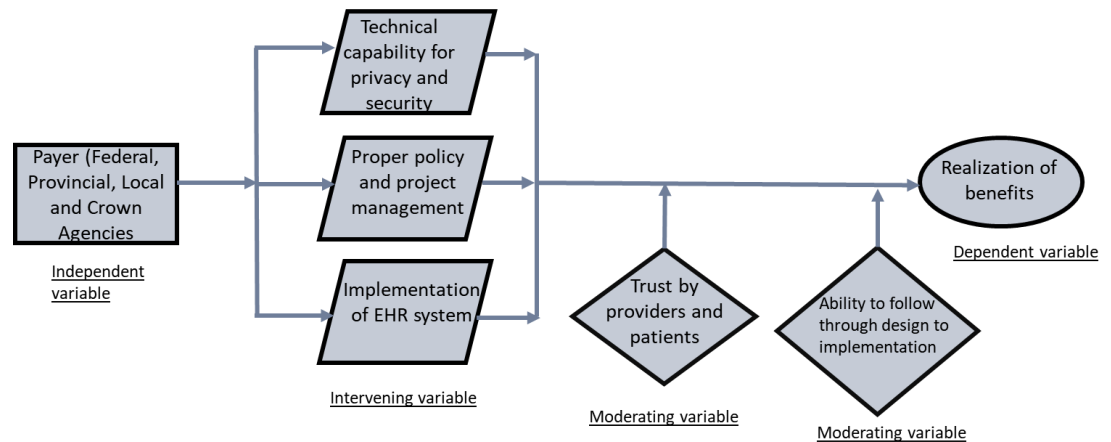


Figure 3-5: Key informant interview framework for payers.

The realization of EHR benefits depends on the payer’s ability to implement technical capabilities to provide privacy and security protection. Increased timeliness of project management will improve the quality and realization of benefits. A higher percentage of completed implementation components of the EHR system will increase the earlier recognition of benefits. The realization of benefits is influenced by the trust of the EHR system by providers and patients. Realization of benefits is affected by the ability to follow through the implementation of EHR systems by payers.

### 3.8 Research Design

Among the 3Ps (Payer, Provider, Patient), the focus of this research is to study the attitudes of patients in their EHR privacy concerns. The findings from payer and provider compared to and used for uncovering knowledge that influences the attitude of the patients.

There are four major types of mixed-method designs. They are the triangulation design, the embedded design, the explanatory design, and the exploratory

design. “In an embedded design, the researcher simultaneously or sequentially conducted the collection of data with separate data analysis and the use of supporting data before or after the major data collection procedure.” (Creswell *et al.*, 2003 p.72). In an explanatory design, the researcher performs the research in phases. For example, phase one quantitative data collection and phase two qualitative data collection that builds upon phase one’s result for the main purpose of testing or measuring qualitative exploratory findings. “In an exploratory design, the researcher does the similar procedure as the explanatory design, except it is for quantitative result” (Creswell *et al.*, 2003 p.72).

Triangulation design is the most common and well-known approach to mixed methods. The objective of triangulation design included using the data to address program objective and program development and evaluation (Creswell, *et al.*, 2003). By utilizing a triangulation design, one can obtain different but complementary data on the same topic to understand the research problem (Morse, 1991, P.122).

### **3.8.1 Patients**

Survey methods were used to measure patients’ attitudes towards privacy and data sharing. The Smith, Milberg and Burke Concerns For Information Privacy (CFIP) survey instrument was used to obtain patient attitudes towards the four privacy dimensions that have been validated by Stewart & Segars (2002). The CFIP framework has been widely used, including a study and validation by Angst & Agarwal (2009). Scenario-based survey questions were deployed within the same survey instrument to measure the decision-making preferences of patients.

In addition to other demographic and qualification questions in the survey, a five-point Likert-scale (ranging from strongly disagree to strongly agree) using a modified CFIP instrument focusing on EHR was used. The following survey questions were asked in the four privacy domains in CFIP:

### CFIP: Collection

- (1) It usually bothers me when health service providers ask me for personal health information.
- (2) When service providers ask me for personal health information, I sometimes think twice before providing it.
- (3) It bothers me to give much personal information to service providers.
- (4) I am concerned that service providers are collecting too much personal health information about me.

### CFIP: Errors

- (1) All the personal health information in computer databases should be double-checked for accuracy regardless of the cost to health service providers.
- (2) Service providers should take necessary and appropriate steps to make sure that the personal health information in their files is accurate.
- (3) Service providers should have procedures in place to correct errors in patients' information in a timely manner.
- (4) Service providers should devote the necessary resources, time and effort towards verifying the accuracy of the patients' health information in their computer systems.

### CFIP: Improper Access

- (1) Service providers should devote the necessary time and effort to preventing unauthorized access to personal information.
- (2) Computer databases that contain my personal health information should be protected from unauthorized access regardless of the cost to health service providers.
- (3) Service providers should take necessary steps to ensure that unauthorized people cannot access personal information in their EHR system.



### CFIP: Unauthorized Secondary Use

- (1) Service providers should not use personal health information for any purpose unless it has been authorized by the individual who provided the information.
- (2) When patients give personal information to a service provider for a particular reason, the service provider should not use the information for other unrelated reasons (such as for commercial benefits).
- (3) Service providers should never sell the EHR personal information to other organizations.
- (4) Service providers should not share personal health information with companies unless this has been authorized by the individual, who provided the information.

*(Adopted and modified from CFIP model)*

### Design of study sample and source of data

Population and Study Sample – The population in this research is enrolled from the Greater Toronto Area (GTA) in Ontario. GTA is the most populous metropolitan area in Canada, with a population of 6.1 million as of 2015 (StatCan, 2016). The GTA consists of the City of Toronto and its surrounding regional municipalities of Durham, Halton, Peel, and York regions. The aim was to recruit approximately 300-500 patients – an appropriate sample size for a reliable estimate that would qualify for meaningful sub-groups comparisons. The actual number of patients recruited was 514. Survey participants are individuals living or working in GTA and had seen a doctor or visited a medical service (hospital emergency, clinicians, laboratory tests and pharmacist consultation) in the prior 12 months before taking the survey. They were at or above the age of 18 when they took the survey.

In Angst & Agarwal (2009) study, they used two groups of subjects. Their first group of subjects was participants of an EHR conference. The second group was a sample of people who opted-in to an online survey sample list provided by Zoomerang, an online survey company. In the author's research, the design

is to create a more random sample than the convenience sample used in the Angst & Agarwal study.

*Collection of data* – In addition to face-to-face data collection on the street, a survey invitation card (Figure 3-6) is being handed out in Greater Toronto Area. The card would direct potential respondents to answer the survey online. Street survey participants were recruited in public areas on the streets. Online surveys, which comprise the same questionnaire as the Street survey, were administered over the Internet via a URL link using a survey software called “Opinio” with version 6.2. Before the formal online data collection, a pilot survey of 20 patients was conducted to test the validity of survey design before the general survey was conducted

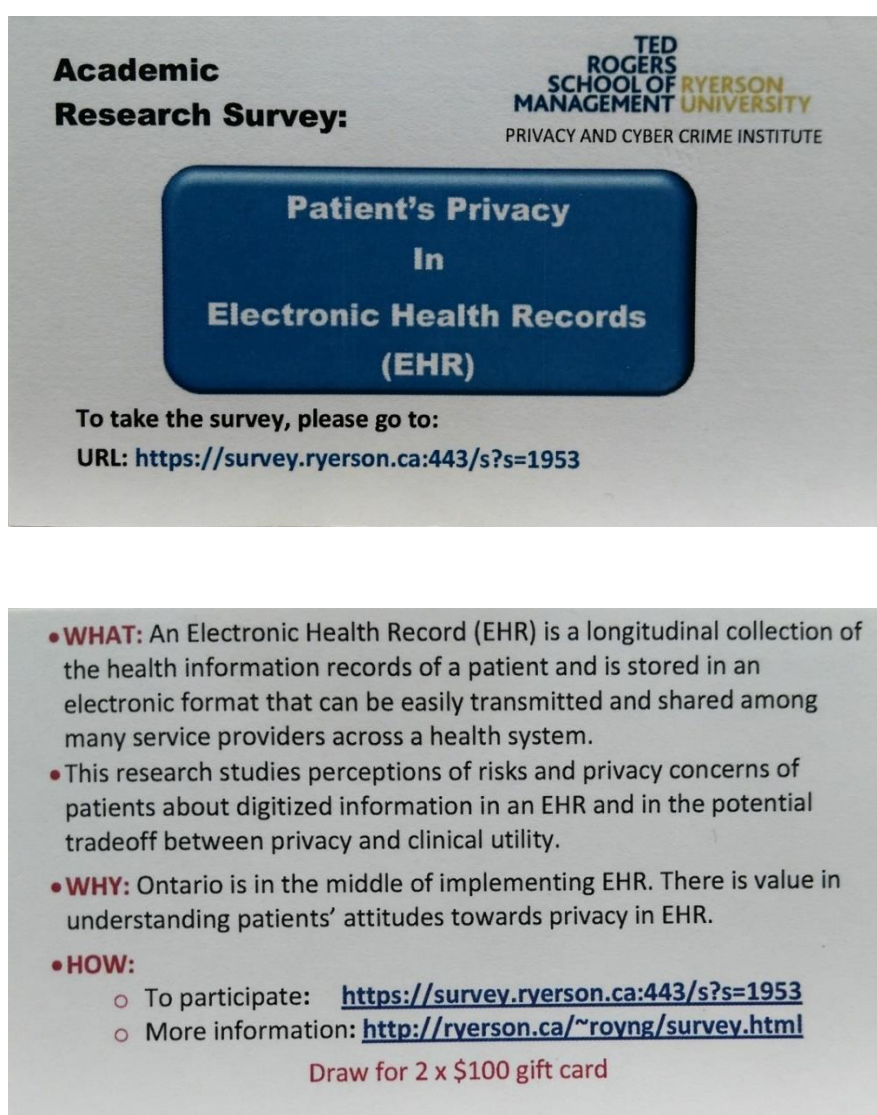


Figure 3-6: Invitation card for online survey

To assess the sub-questions in Chapter Two related to the question: “Is patient’s age group or career stage a factor influencing the level of privacy concerns?” Classroom surveys for students were conducted in an undergraduate program using a convenience sample technique. In addition to the privacy questions to all the patient groups, the author would also like to explore if this younger age group has a stronger willingness to give out private information, as they are savvier and more often using social media, which involves a great deal of information sharing.

*Exposure assessment* – It was expected that due to a very diverse ethnic community in GTA (over 80 languages and dialects spoken in GTA), the terms used in the survey needed to be carefully selected. A glossary of meanings and terms was provided for each particular question that was asked. It was decided that a progress indicator (i.e., number of questions/total questions) would be displayed on the respondent’s computer screen to ensure that respondents would not abandon the surveys before completion.

*Data management* – A master copy of the survey results was first created on another hard disk drive (for permanent records) and set aside as backup and for auditing purposes. A verified copy of the master record was saved in the Microsoft Excel spreadsheet format. It was later inputted into Stata (version Stata/IC 10.1) for statistical analysis.

*Data analysis strategies* – First, standard descriptive statistics software such as Strata as computed and analyzed. Then, based on the results, the appropriate inferential statistical analysis was employed such as Excel spreadsheet with statistical analysis option added.

*Ethics Review Board approval* – The Ethics Review Board approved this research study (with the proposal, a guide to the field and online survey and survey forms) from Ryerson University, Toronto, Canada.

### 3.8.2 Providers

Providers refer to licensed professional who provides medical care to patients.

Three nurses and two pharmacists participated in focus group one, and one general practitioner, one radiologist doctor and three hospital-based doctors in focus group two. To establish a baseline of knowledge and understanding of the research, the focus groups participants were sent with a list of questions before attending the discussion session.

The following five questions were emailed to the two focus group participants.

1. What are the perceived risks around the sharing of private/sensitive personal information with healthcare providers when information is shared across EHR system?
2. What EHR information do providers need to deliver effective care?
3. What patient private information do physicians need to know, from primary care to emergency care? (The purpose is to perform sub-group analysis to correlate with patient's change of willingness to evaluate if there is a difference)
4. What information do pharmacists need when considering the effects of drugs before a prescription is dispensed?
5. Is there any critical information even the provider would not want to share in the system?

Noting the comments and themes that emerged during the discussions, semi-structured discussion techniques were used. A free flow of discussion with a set of open questions was conducted after the following questions were first addressed to each participant.

*Population and study sample* – The population demographics covered the Greater Toronto Area (GTA). Service providers in this study are those currently licensed to practice in the province of Ontario and are performing their work within the GTA.

*Source of data* – The study sample of providers included three nurses, two pharmacists, two clinicians, and three radiologists. Participants are randomly recruited from public published directories of their respective professional organization such as the Ontario Medical Association, hospitals, clinics or public speaker profiles.

*Exposure assessment* – It is expected that focus group participants are very busy medical professionals. They plan for recruitment was to use postal-letter, or an email sent directly to their office or their email address. A pre-arranged schedule and at a formal research study studio at Ryerson University was used. Due to the providers' busy schedule and the difficulty for an arrangement of common time for discussion, if necessary, outside recruitment firm may be engaged.

*Data management* – As per the research proposal, a video camera was used to record the discussion during the session. A tape recorder was mandatory and used as a backup tool to capture data. Also, the focus group discussions were conducted in a proper research boardroom with pre-installed cameras and a camera-switching system to record the entire meeting without distracting nor interfering with the flow of the discussion. These interviews were taped, transcribed verbatim and analyzed using various software such as NVivo version 9, Microsoft Office Excel 2013 spreadsheet and Leximancer version 1.2.

*Ethics and human subject issues* – As the research is conducted in the province of Ontario and is supported by the Privacy and Cyber-Crime research institute at Ryerson University, the research data-gathering proposal and the research survey instruments were carefully reviewed and approved by Ryerson University research ethics board. This research ethics board uses the Tri-Council (Canadian Institute of Health Research; Natural Sciences and Engineering Research Council of Canada and Social Sciences and Humanities Research Council of Canada) standards and policy statement to evaluate the fulfillment of research ethics standards. The survey forms and its contents have been reviewed to meet the council's standard of research ethics requirement. As it is a research study done locally in Toronto, Canada and is receiving

comprehensive approval on research ethics using tri-council standard, there was no requirement for research ethics approval from The University of Manchester. In addition to the research surveys, Focus groups and key informant interview guides were also reviewed by ERB for ethics approval.

### **3.8.3 Payers**

Key informants in this research are payers of the EHR system or key stakeholders such as experienced founders of similar EHR system, leaders from the medical association or legal experts with experience in electronic health records. The purpose of key informant interviews is to collect expert information from a wide range of people who have first-hand knowledge regarding the use, design, and implementation, costs, and expectations of the EHR system. They can provide particular expertise and understanding of management issues, and insights on the nature of problems and give recommendations for solutions. In order to achieve no cross-influence with the presence of another informant, each key informant was interviewed individually.

The following nineteen statements with a 5-level Likert scale rating were asked to the key informants who are closely responsible or knowledgeable for the EHR system and are considered as subject matter expert. These questions are adopted from the published benefits at the beginning from the EHR initiative. The purpose is to solicit evaluation and opinions now that many EHR sub-systems were implemented.

1) EHR implementation will improve the quality of care of patients
2) EHR implementation will improve the consistency of care of patients
3) EHR implementation will allow timely access to comparable data from multiple sources such as hospitals
4) Use of standardized health information will allow for faster review of health information
5) Increased use of measurable health information rather than free-text only found in the paper record
6) Reduced reliance on verbal exchanges of health information between provider and patient
7) Reduced reliance on anecdotal (based on personal experience or reported observations unverified by controlled experiments) exchanges of health information between provider and patient
8) More accurate communication among (health service) providers
9) More effective communication among (health service) providers
10) Reduced duplication of effort in prescribing tests
11) Better ability to consolidate clinical findings
12) Shorter elapsed time between steps in the healthcare process
13) Higher probability of positive patient treatment outcomes
14) Higher probability of positive patient satisfaction
15) EHR helps the government to reduce rising health costs (such as duplication of a lab test, patients doctor hopping)
16) Shorter elapsed time between steps in the healthcare process
17) The security of personal health information will improve with EHR
18) There will be better patient privacy protection with EHR
19) There will be better protection of doctor-patient confidentiality with EHR.

Table 3-1: Published benefits statements from EHR initiative

*Population and study sample* – The population of key informants was drawn from payers of the health systems such as the provincial government, infrastructure experts in EHR implementation, and officials from the local health associations. Examples include officials from the federal government, the provincial government and a crown agency. Also included were subject matter experts involved with EHR initiative in Canada.

*Source of data* – The payers and subject matter experts were identified using a public government directory, professional organization's directory, hospital directory or public presentations that contain the participant's contact information. Phone calls or email were used to introduce the research study and schedule appointments for potential participants after an invitation letter was sent out to them.

*Collection of data* – Eight individual meetings were conducted with each key informant one at a time, and data was collected using the audio taping technique with prior agreement. Findings of the key informant groups were used to explain the patient's concern about privacy in the EHR system.

*Exposure assessment* – It was expected that due to the busy and unstable working schedules of some participants in the payer's group, a pre-arranged or agreed upon schedule and a convenient location had to be used.

*Data management* – Permission was received to use a voice tape recorder as a backup or primary device to capture the data for the payer group. The voice data were transcribed verbatim into a written format with thematic coding. Participants were given the opportunity to review their transcribed interview before accepting as verified research data.

To assess the effect of the implementation of the EHR project separately, the author conducted two provider focus group interviews and a full patient group survey after the initial data gathering from key informant group. These three groups of data collections set up the foundation of dialectical method of analysis using the thesis, antithesis and synthesis triad in Chapter Seven.



### **3.9 Synthesizing and Validating the Findings Using Triangulation Design**

Among the 3Ps (Payer, Provider, Patient), the focus of this research is to study the attitudes of patients in their privacy concerns in EHRs. The findings from payer and provider are synthesized to and used for uncovering knowledge that supports the findings of the patients.

Extending the discussion on Triangulation design in section 3.8 (Research Design), the validity of findings can be increased when different and independent data are supporting the results. The author uses triangulation of three sets of data to assess (using other instruments from focus groups and key informant interviews) the findings from the patient's survey.

It is the opinion of the author that while the use of the triangulation design techniques may increase the validity of the findings, there will always be some extraneous factors that are not observable from the research data and that may contribute or influence the results.

Referring to the diagram below, and based on the three different instruments (Key Informant Interview, Focus Group, and Survey), three independent sets of data are obtained. There are primarily three "types of findings" that can be influenced by the evidence. They are:

(a) Type 3 finding --- Findings is based on (or be traced back to) evidence from data obtained from all three groups of subjects. They are Patients, Providers, and Payers. A type 3 finding has the most robust validity because it is supported from the data evidence with three different types of research instruments (Survey, Focus Group, and Key Informant Interview) from the three different subject groups (3Ps).

(b) Type 2 finding --- Finding is based on (or be traced back to) evidence from data obtained from any two of the three groups of subjects. A type 2 finding has good validity because it is supported from the data evidence with any two of the three different types of research instruments (Survey, Focus Group, and Key Informant Interview) from the three different subject groups (3Ps). In addition

to the core group findings on the patient, a type 2 finding can also be a finding on the provider or payer group that has evidence from the other 2Ps.

(c) Type 1 finding --- Finding with evidence came from a single-Level (that is its own P). The single level finding can be from patient, provider or payer. If it is a patient's type 1 finding, it shows a valid result based on the research method and is part of the core findings of this research. A type 1 finding on privacy issue is part of the core research findings as sub-research question have defined the intent to explore such area. A type 1 finding is not part of the core research exploration but can be a contributive finding that is found as a by-product of the research study. It is noted that a type 1 finding is a good start for next research to expand understanding of forces and attitude that have not been covered in the scope of this research.

Types 1 to type 3 findings are of contribution to answering the research questions or describing some constructs such as benefits, efficacy, countermeasures, and risks. The following figure shows how the Triangulation design was used to correlate the relationship of evidence to findings via the three types of findings in Chapter Seven.

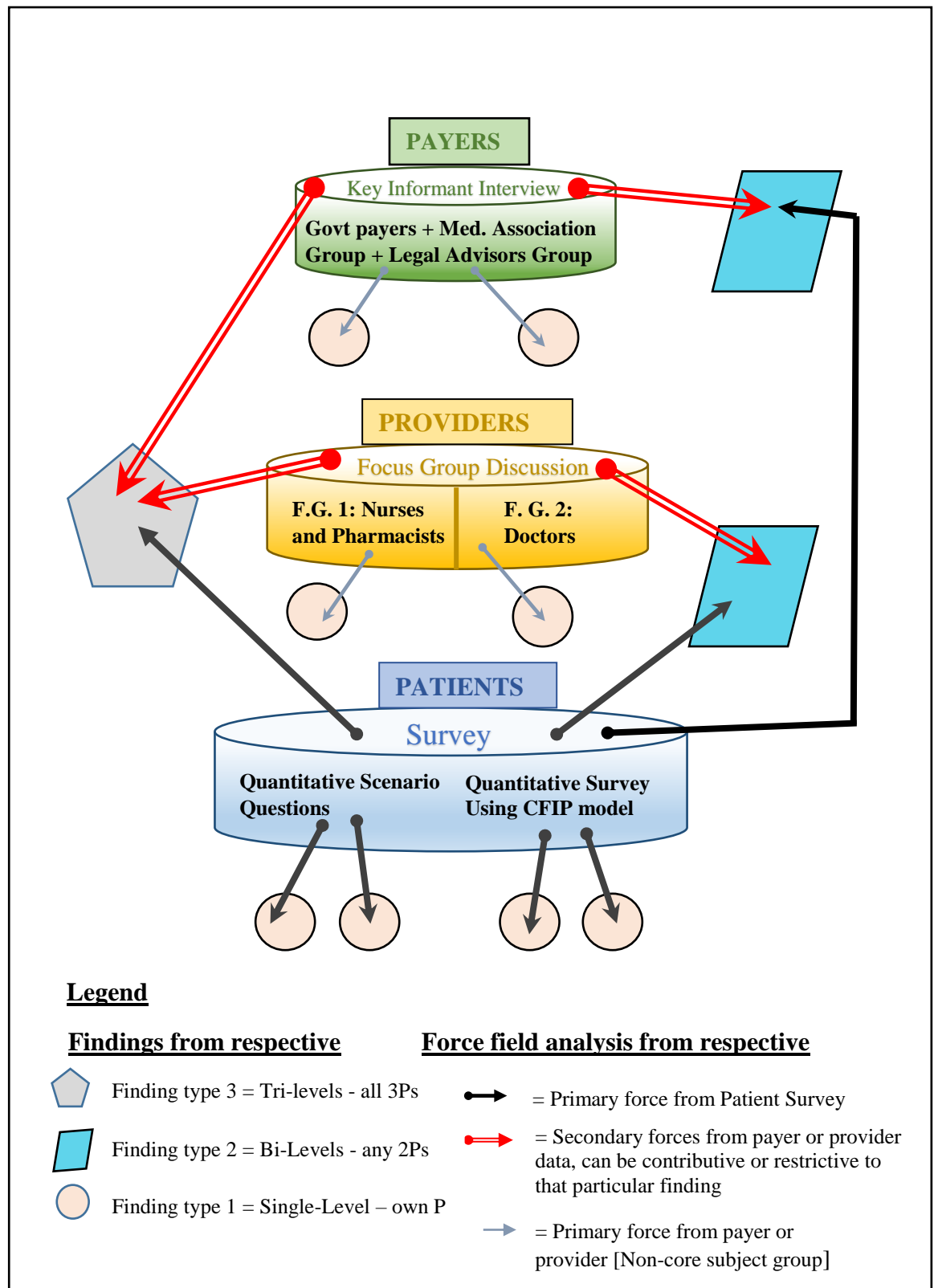


Figure 3-7: Types of findings from a Triangulation mixed method design

### **3.10 The justification for Human Involvement**

Privacy concerns arising from the introduction of Electronic Health Records or its component functions are experienced by patients. Only through interview and survey involving humans the author was able to obtain the perceptions of these human subjects. Previous traditional privacy surveys using the CFIP instrument developed by Smith, Milberg, and Burke (1996) and modified by Stewart & Segars (2002) all used humans in the research.

### **3.11 Study Location**

Key Informant Interviews were conducted either at the participant's office or at the Ryerson University. Both locations of the interviews were in a private room. Focus Group discussions took place at Ryerson University Ted Rogers School of Management building in a private room. Street Survey participants were recruited from public areas on the streets. Online Internet surveys were conducted over the Internet web-browser using a Uniform Resource Locator (URL) link.

### **3.12 Chapter Summary**

This chapter set out to provide a philosophical discussion and framework in guiding the research methodology. The research method, models, and designs are discussed. Triangulation design is used to synthesize and validate findings from patient surveys against data sets from providers and payers. This triangulation of data will help to understand how the implementation of the EHR and the evaluation of the program result on the patients' concern about EHR system. This chapter lays the foundation that guides the planned method, procedure, and process of this research study. It also set the direction and guiding principle for the later chapters with the collection and data analysis for the 3Ps resulting in the uncovering of insights and findings from this research.

## Chapter 4 Results of Patients' Survey

### 4.1 Introduction

The focus of this research is to study whether patients in Greater Toronto Area have significant concerns about privacy in EHR by studying their attitudes and their willingness to provide sensitive and private information for the EHR. This research also examines whether patients exhibit behavior similar to patients in the USA in their evasion of privacy exposure within their EHR. According to the review of literature in Chapter Two, patients in the USA have taken evasive actions and countermeasure that result in the reduction of efficiency and efficacy of the Electronic Health Record system (Health & Medicine, 2006). Studying Canadian patient attitudes towards their concerns about privacy in EHR helps to understand the acceptance and the quality of services to patients in the EHR system in Canada.

Guided from the perspective of a critical realist, the author believes that patients' concerns can be the result of their formed attitude. This formed attitude is influenced by a patient's perception and experience when interacting with service providers. Very often, such experience comes from patient's encounters with the service provider that uses the EHR. It is suggested that a person's behavior is a complex issue that can be linked to perception and the social environment (Bargh, *et al.*, 1996, Chartrand, *et al.*, 1999). Such perception is not necessarily the actual reality or the truth. Similar to the arguments in "Perception and Reality" presented by Keith Wilson (2013) in that pervasive perception is susceptible to illusion using our human-sensory. While patients may perceive, in their judgment that a certain aspect of EHR is negative to their benefits, the same aspect is welcomed as a positive contribution to the EHR system by the payer. The author suspects that this seemingly oxymoronic and contradictory nature of the perception and reality can be explicated with the proper context as an unobservable event that was not revealed during the

experience of the patient-provider engagement. It is important for this research to study patient attitudes and how the “behind the scene” factors, such as design and policies from payers and the practice of the provider can influence patient attitudes. We facilitate a holistic view of the matter by surveying the patients, discussion with providers and interviewing with the payer. This holistic approach helps to identify the gap between the patient’s perception and the actual design or practice of the ERH system. One of the goals of this research is to understand if such a gap can be narrowed by increasing awareness and communications from payer or provider to patients.

A survey instrument is used to study the patient’s attitude. Twenty-six explanatory variables were used with one moderating variable DSP (Believed that data can be secured and private) and one explained variable WIW (Willing to provide more information if sickness worsens). The DSP moderating variable is used to investigate a patient’s perception of trusting the EHR system through their experience with the service providers. The WIW is a response (dependent) variable. It is also used to investigate if any force is at work (in this case, worsening of sickness) in the trade-off between withholding and willingness to provide private information that the patient was not willing to provide before the deterioration of the patient’s health.

This chapter provides the results of the survey and initial findings. A separate discussion chapter, Chapter Seven, will present overall analysis and discussion after results of focus group discussion with a service provider in Chapter Five and result of key informant interview with payer in Chapter Six.

Section 4.2 discusses the patients three sampling groups and how the convenience sampling group is statistically different and therefore should not be combined with the street and online survey group. Section 4.2.5 outlines the justification and the formation of two sample groups (group1: street and online group and group 2: student group). The aggregation of data from groups is possible as the same survey questionnaire is used for each group. Section 4.3 describes the three validity methods to validate and assess the reliability of the survey instrument. Section 4.4 provides descriptive statistics on the survey result on patient concerns and outlines the justification and the formation of two

sample groups (group1: street and online group and group 2: student group). Section 4.5 reported the result of the four CFIP dimensions. Section 4.6 to 4.8 describes the age, career stage, and gender of the survey respondents. Sections 4.9 to 4.10 describe the qualitative result on scenarios. Section 4.11 to 4.13 presented the emerging themes and preliminary findings. Section 4.14 summarizes the results, providing a foundation for the discussion in Chapter Seven.

## **4.2 Survey to Study Patient Attitudes**

Since individual patients have different attitudes based on their experiences and values, the choice of a survey as a research instrument is appropriate and is a common tool to collect data relating to attitudes and opinions. To measure the different degree of the firmness of the participant's opinions (attitude measurement), an ordered categorical survey was designed to capture the varying degree of firmness of the patient's attitudes towards sharing information with healthcare providers.

### **4.2.1 Sampling Groups and Triangulation of the Survey**

To assess patient concerns in the Electronic Health Record in Ontario, three different channels to collect the survey data were used. They were a street survey, Internet online survey and classroom survey. The street survey allows random and face-to-face clarification of questions during the survey. Online survey supplements the geographical coverage of the Greater Toronto Area that cannot be covered by the street survey. Classroom survey of students is a convenience-sampling group that can obtain data from a younger demographic (mostly 18 – 25 years of age). These students are enrolled in an information technology undergraduate program. The purpose of surveying this younger age group is to examine whether this younger age group has a greater willingness to



give out private information, as they are more computer and information technology savvy. This student group is accustomed to texting from their mobile devices and commonly upload their personal information to their peer group using social media.

The street, online and classroom samples of the survey allow for a triangulation validation within the same survey instrument. 131 street survey questionnaires were completed of which 115 were accepted as valid (qualified) for the research study. Some forms were completed, but the respondents did not meet the qualification as a GTA patient within the survey criteria. 118 online survey questionnaires were collected of which 86 were accepted to the research study. For the convenience sample method of classroom surveys, 264 questionnaires were completed of which 252 were qualified and admitted for the research study. Since the three samples used the same questionnaire, the effect of the questions asked can be studied by adding the three samples together if they meet the statistical check. The total number of questionnaires collected was 513 of which 453 (88.30%) were accepted as useful for data analysis.

Sample	Design/ Purpose	Purpose	Form completed	Useable form	Male	Female
<b>Street Survey</b>	Random	Provide resemblance of populations	131	115	45	70
<b>Online Survey</b>	Random with expanded geographical coverage (GTA)	Provide resemblance of populations	118	86	40	46
<b>Classroom Survey</b>	Convenience sample with mostly younger age group (18 -25)	Investigate younger age patients who usually are much computer savvy	264	252	168	84
		TOTAL:	513	453	253	200
		("Total/453*100) in %		100%	55.9	44.1

Table 4-1: Description of the three samples of the same survey questionnaire.

#### **4.2.2 Structure of Questionnaires**

The survey questionnaire composed of four parts (see Table 4.2 below). Part “Pre-” asked two questions to qualify the respondents for the survey. Part 1 asked the demographics of the respondent. Part 2 is composed of fifteen questions (act as predictors in the survey) which is divided into four areas of concern aligning to the “Concern for Information Privacy Model (CFIP)” developed by Smith *et al.*, (1996, p.172). The four categories are Collection; Unauthorized Secondary Use; Improper Access and Errors. Also, two response variables in the survey were added to measure the patient’s overall attitude. Each question contains a five-point Likert scale that is constructed to be an ordered categorical scale. Part 3 includes a series of five scenario questions to study if patients will have a utility trade-off of their privacy if their health is worsened.

Parts	Categories of concerns	Variable	Description
Pre-	Qualification of respondents		Live or work in GTA?
			Visited a doctor in the last 12 months?
1	Demographics	AGE	Age
		SEX	Gender
2	Collection (too much)	BGI	Bother me when I give info
		TTD	Think Twice before Disclosure
		BMI	Bothered when too much Information collected
		MIC	Too much info. collected
	Error in records	ARC	Accuracy regardless of cost
		NSA	Necessary step to ensure accuracy
		CET	Correct error timely
		VAI	Verify accuracy of info
	Improper Access	EUA	Efforts to Ensure Unauthorized
		DPU	Data protected from unauthorized
		PUA	Prevent unauthorized access
	Secondary use	NOP	Use for no other purpose
		NOU	No other use
		NSI	Never sell EHR info.
		NUS	No unauthorized share of info
3	To assess patient's reaction to a given scenario	SSWC	Scenario: Provider Shared info without concern
		SDSR	Scenario: Disclose info. will result Social Rejection
		SDFL	Scenario: Disclose info. will result Financial Loss
		SDWE	Scenario: Disclose info. when in emergency
		SDWC	Scenario: Disclose info. but With Countermeasure

Table 4-2: Structure of the questionnaire and a brief description of the variables

In addition to the above four categories of predictive variables, one modulating variable DSP and one response variable WIW is included in the questionnaires. The meaning of these variables is listed in the following table.

<b>Modulating variable</b>	DSP	Believe that Data can be Secure and Private
<b>Dependent (response) variable</b>	WIW	Willing to provide more information if sickness worsens

Table 4-3: Modulating and response variable with a brief description

#### CFIP Factors Based Survey: Patient willingness to provide health information

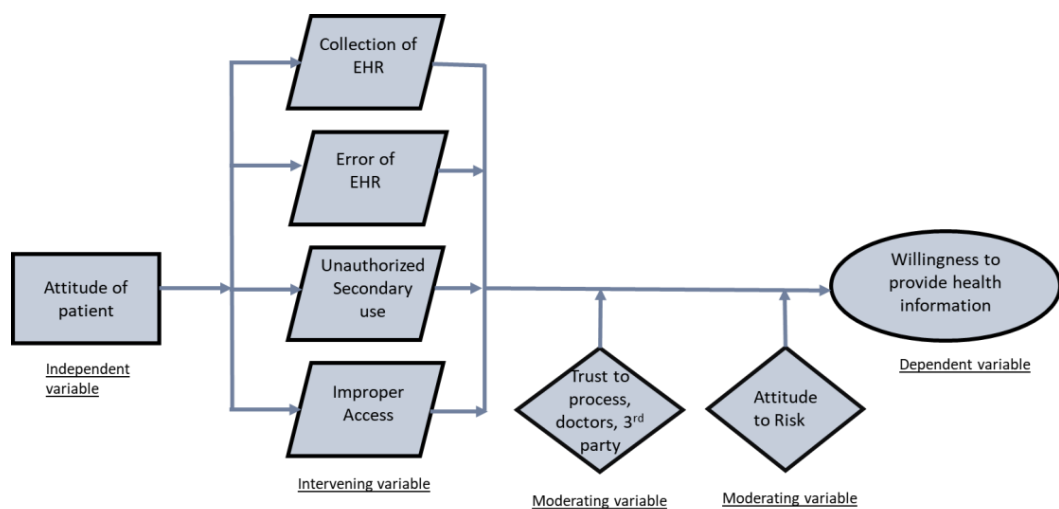


Figure 4-1: Qualitative survey framework for the patient.

The main portion of the survey is in part 2. It measures patient's perceptions and concerns of their privacy of digital information held in an EHR. In measuring attitude, Likert scales are commonly used. This research employs a typical five-level Likert item which ranging from "strongly disagree" to "strongly agree." The statements in each question provide a positive and negative range of views, sentiments or opinions.

The properties of a Likert scale are the use of "a series of verbal statements that expressed a range of positive expressions, views, sentiments, claims or opinions about the "attitude object (under construct)" that ranged from mildly positive to strong positive with similar negative range of the opinion" (Carifio & Perla, 2007, p. 113).

With a set of five Likert items (choices) representing the different degree of positive and negative positions away from the “Undecided” (third category) in the scale, this forms an ordinal scale which is classified as categorical ordered variables in the survey.

#### **4.2.3 Data Integrity and Cleaning**

In this research proper coding and cleaning is required to ensure that when performing the inferential statistics, redundant or non-contributive parameters are removed to provide relevancy of the statistical result. For example, the Likert item of “Neutral” coded as “3” will not contribute to inferential, as it does not present an increase or decrease of the patient’s attitude towards the privacy concerns of Electronic Health Record.

#### **4.2.4 Survey Instrument**

Each survey form used, whether it is for street survey or classroom survey are all serialized and reviewed for completeness and accuracy before accepting into the research database.

For the online survey, a software program called “Opinio” with version 6.2 was used to create the webpage and manage the online responses. It also produces a text format of the received data which can be readily assimilated by other data. For the street and classroom surveys, paper questionnaires were used. When the survey was completed, the data from paper questionnaires was extracted and was coded into an Excel spreadsheet in text format. It was later imported into Stata/IC 10.1. Stata is an integrated statistical software package that provides data management, data analysis, and graphics.

Visual inspection of data completeness and sample verification of forms to data entry correctness were checked. There were cases where some forms had

scenario sections not answered. There were also cases where selectively, some questions were not answered by the respondents. A careful review of this incompleteness and they were all accepted as the respondent may not be willing to answer a particular question. It does not affect the outcome as the statistical calculation is based on per question and is relative to the total number of respondents answering that question.

Missing data is coded with “.” before running the Stata statistical software to ensure that Stata acknowledges that the particular field has a missing response. In doing so, an incomplete survey form was still useful. This allowed the accommodation of the respondents in the preservation of their freedom in answering the question.

#### **4.3 Validity and Reliability of the Survey Instrument**

Validity is defined as the extent to which a concept is accurately measured in a quantitative study (Heale and Twycross 2015). Bryman and Bell (2007, p.733) defined “Validity as a concern with the integrity of the conclusions that are generated from a piece of research”. They further elaborated validity refer to the issue of whether or not an indicator (or set of indicators) that are devised to gauge a concept really measure that concept (p. 165). Creswell (2005, p.600) stated: “Validity means that researchers can draw meaningful and justifiable inferences from scores about a sample.” Creswell further suggested that a researcher should examine whether the instrument selected for use in the research study yields a score that is valid. In this chapter, the author will first examine three common types of validity (Content, Criterion, and Construct) and then with other validity measurements. It is then followed with a discussion of the established validity in the “Concern For Information Privacy (CFIP)” model that has been validated as a standard measurement in the assessment of privacy using survey, and then further examine the internal reliability of the survey instrument. In the sequence and type of validity, most validation studies begin by assessing Content Validity, then the criterion validity and then followed with

the construct validity (McDowell, 2006 p. 30-34; Creswell, 2005 p.165). Although there are other types of validities such as factorial validity; discriminatory validity and predictive validity, the author used the relevant types of validity towards this paper and also follows the above mentioned conventional practices by examining the following validities.

#### **4.3.1 Content Validity**

Content Validity concerns itself with the comprehensiveness and the representation of the possible questions and the relevance to the concepts being measured (McDowell, 2006; Creswell, 2005). In this study, the quantitative survey measured the four dimensions of privacy in the CFIP model by adopting the questions within each of the four selected dimensions. They are Privacy Concerns: 1. Unauthorized Secondary Use of Information; 2. Improper Access; 3. Information Errors, and 4. Too Much Collection.

According to Nunnally (1978, p.92): “The two major standards for ensuring content validity are: (1) a representative collection of items and (2) “sensible” methods of test construction. To substantiate the content validity, the author has used the following two procedures:

(1) Using multiple questions --- Within the same privacy dimension in the CFIP models, multiple questions were used to increase variety and coverage of possible questions within the same concept (privacy dimension). For example, in the privacy dimension of “Privacy Concerns on Unauthorized Secondary Use of Information” four questions were asked to encompass comprehensiveness of this dimension. They are:

- (a) Service providers should not use personal health information for any purpose unless it has been authorized by the individual who provided the information.
- (b). When patients give personal information to a service provider for a particular reason, the service provider should not use the information for other unrelated reasons (such as for commercial benefits).

(c) Service providers should never sell the EHR personal information to other organizations.

(d) Service providers should not share personal health information with other companies unless it has been authorized by the individual who has provided the information.

Similarly, there are four questions in the privacy dimensions of Information Errors and Too Much Collection. There are three questions in the Improper Access. As evidenced by the variety of the four questions in the privacy dimension of Concern of Unauthorized Secondary, these questions covered the areas: No unauthorized use for other purpose [variable NOP]; Not to use for unrelated reason [variable NOU]; No selling to third parties [variable NSI] and finally, and No unauthorized sharing of the information [variable NUS]. These questions covered four different aspects of the privacy concerns on the unauthorized secondary use of information. Based on the literature on the evidence to substantiate for content validity (Bryman & Bell 2007; McDowell, 2006; Creswell, 2005) and in the opinion of the author, the use of face validity techniques and multiple questions to cover the comprehensiveness and the representation of the possible questions which appear relevant to the privacy dimension being measured can be served as evidence that contents validity is achieved.

(2) Using Face validity to check if questions make sense --- Face validity often used for finding out if the questions in the survey make sense. The standard practice is to ask the experts or knowledgeable persons to review if questions make sense. The author has asked researchers from Toronto, working at Sick Kids Hospital and three research assistants to review and examine the measures used in the survey is sufficiently reflect the contents of the concepts used in the four privacy dimensions in this research study. Also, from a patient point of view, a small sample of four patients was asked to review the clarity of the contents, and comments on their assessment of the survey questionnaires to reflect if the question asked in the questionnaire would solicit their appropriate response to the four privacy domains in this research study. The result is a positive response in the understanding and clarity of the questions that allow the



measurement of the privacy concerns in this study. It is also noted that the questions are adopted from a validated research measurement in Smith, Milberg and Burke's CFIP models (1996).

#### **4.3.2 Criterion Validity**

According to Garrison (2016, p23) "Criterion validity has to do with the correlation between the scale of interest and known and established and accepted standard measures for the same construct. Criterion validity defined this way is also called concurrent validity."

##### **4.3.2.1 Concurrent Validity**

Smith *et al.*, (1996) in their paper on CFIP model has an illustrated concurrent validity on three questions from previous public opinion surveys were used. The result was a correlation between each subject's response to these three questions are 0.35, .36 and .46. The author uses the dependent variable DSP (I think that service providers can keep my data secure and private against the concurrent questions on independent variables NOU (No other Use); VAI (Verify accuracy of Information); BGI (Bothers me when giving information) and BMI (Bothers me when too much information is collected).

It is expected that NOU and VAI has a positive correlation, as a criterion to DSP and that BGI and BMI has a negative correlation, as a criterion to DSP. This is because of the stronger the score of BGI and BMI the more negative the attitude (it bothers me) to the DSP in that question.

The author used the randomized sample from the "Online and Street" to measure the concurrent validity instead of the convenience (possible biased) sample of classroom student survey.

The result of the correlation of DSP among the other four variables as listed as follows.

Correlation:	DSP
NOU	0.2378
VAI	0.2199
BGI	-0.2520
BMI	-0.2451

Table 4-4: Correlation of DSP among the other four variables

The result of the concurrent validity is comparable to Smith, Milberg & Burke's values

### 4.3.3 Construct Validity

Construct validity is defined as the degree to which an empirical measurement or hypothesis testing of a construct is validly measuring what it purports (claim) to measure of the theoretical concept (Thatcher, 2010; Smith, Milberg & Burke 1996). In this research, a single key construct of "privacy" is measured with 15 surveys items form four CFIP dimensions. In the qualitative study using focus group and key informant interviews, triangulation design is used.

"Triangulation is a validity procedure where researchers search for convergence among multiple and different sources of information to form themes or categories in a study (Creswell & Miller 2000 p.126)."

"Internal consistency is a type of convergent validity which seeks to assure indicators measure a single construct. Cronbach's alpha is commonly used to establish internal consistency construct validity for similarity scales, with .60 considered acceptable for exploratory purposes, .70 considered adequate for confirmatory purposes, and .80 considered good for confirmatory purposes. Cronbach's Alpha is both a validity coefficient and a reliability coefficient." Garson (2016, p.15).

The following table shows the convergent validity as evidence of the construct validity by using the Cronbach's Alpha. The author has computed the Alpha from this research study and referenced it to those from Smith *et al.* and Angst & Agarwal's studies.

Convergent Validity (Internal consistency)	Cronbach's Alpha		
	From this research	From Smith, Milberg & Burke's (1996) paper on CFIP model p.185	From Angst & Agarwal (2009) paper p.269 Table B1
SECONDARY USE	0.914909	0.88	0.82
IMPROPER ACCESS	0.635967	0.75	0.90
ERRORS	0.727863	0.84	0.84
COLLECTION	0.836943	0.88	0.64

Table 4-5: Convergent validity of this study using Cronbach's Alpha

Based on Garson's statement above, the construct validity in this research using the Cronbach's Alpha assessment suggested that "Secondary Use" dimension has the most robust validity. All three other CFIP dimensions are comparable to the other two publications above that also used the same CFIP dimensions and similarly adopted survey instrument.

#### 4.3.4 CFIP Model: A Validated Instrument for Research on Information Privacy

Smith, Milberg & Burke (1996) proposed a privacy model and a validated instrument that has been used, extended and accepted by other scholars. The research study from Smith, Milberg & Burke (1996) was to create a validated research instrument with validation by conducting and measuring of "Individuals' Concerns About Organizational Practices."

Smith *et al.*, have stated their objective was

To enable future studies in the information privacy research, we developed and validate an instrument that identifies and measure the primary dimensions of

individuals' concerns about organizational information privacy practices. (Smith *et al.*, 1996. p 167)

The CFIP model has been used in research paper on topics such as Measuring Mobile Users' Concerns for Information Privacy (Xu *et al.* 2012); Extended in Internet Privacy Concerns (Hong and Thong, 2003), and in the Adoption of Electronic Health Records in the Presence of Privacy Concerns (Angst & Agarwal, 2009). The author of this research study uses this CFIP model and the same four CFIP dimensions as it is also used by the above researchers and are well accepted by the research community as a validated instrument.

#### **4.4 Descriptive Statistics of the Survey**

As described in Table 4.1, there are three different samples conducted using the same survey questionnaire in this study. They are online survey; street survey, and student classroom survey. By using a five-level Likert scale to measure the answers from respondents, the study of respondent's attitude is recorded. These answers are enumerated most effectively by presenting in the frequency of the answer to the question asked. The following describes the data collected.

Out of 513 survey forms completed, 11.6% (60 out of 513) were not admitted to the research database, as the respondents did not meet the criteria required for the survey. These criteria require the respondent: to have visited a doctor in the last 12 months and working or residing within the geographical research area of the Greater Toronto Area (GTA). An accepted respondent who has met these criteria is qualified as a patient in this study. Of the sample population of 453 accepted respondents, there are 253 (55.8%) male and 200 (44.2%) female.

Of the 453 usable survey forms, 86 were enumerated from an online survey, 115 from street survey and 253 were from classroom student survey. It is noted that even though the classroom survey is drawn from random classes as it becomes available, its mean value is significantly different from the online and street

survey. Table 4-7 and 4-8 below provide the result of Analysis of Variance (ANOVA), which confirmed that classroom survey is statistically different in its estimated population mean from that of the online and street survey's estimated population means. It is, therefore, treated as a sample from a different population and the description of this group (classroom survey) is done separately from that of the online and street survey group. By only performing an analysis of variance on the two remaining samples Table 4-8 confirmed that the online and street survey sample has a similar estimated population means and they are statistically related. They can be used to estimate or describe the same population. Therefore, further analysis will combine the online and street survey into one sample and rename as online and street sample (O + S) group when appropriate. Two hypotheses are set to test for the relationship of the sample means to consider if the samples could describe the same populations. The hypotheses are:

**Null hypothesis  $H_0$**  = means of the three groups are the same mean (online) = mean (street) = mean (classroom)

**Alternative hypothesis  $H_1$**  = means are different.

The rejection region for the null hypothesis is a p-value of less than 0.05. It implies that there is less than 5.0% in the probability that the null hypothesis  $H_0$  is true. In Table 4.7 below, if  $H_0$  is rejected, it implies that at least one of the mean is statistically different from the other means within the  $H_0$  statement. Therefore, the values of the three samples cannot be added up together to be analyzed as one unit that came from the same population.

The result presented in Table 4.7 below shows that there is a significant variation of the sample mean among the three groups. With a p-value of less than 0.05, there is a less than 5.0% probability that the means of the three samples under calculations are statistically related. Therefore, these three samples: online, street and classroom samples cannot be treated as coming from a similar population. The values observed in these three sample groups cannot be aggregated together to form one sample. From Table 4-8, the result of ANOVA calculation shows that many of the variables are with  $H_0$  rejected.

Below is a full summary table of all the variables for the four CFIP dimensions with one-way analysis of variance (ANOVA).

In the followings, Table 4-6 provides the legend to each variable that is used in Table 4-5 and Table 4-6 in the ANOVA results.

Collection (too much)	<b>BGI</b>	Bother me when I give info
	<b>TTD</b>	Think Twice before Disclosure
	<b>BMI</b>	Bothered when too much Information collected
	<b>MIC</b>	Too much info. Collected
Error in records	<b>ARC</b>	Accuracy regardless of cost
	<b>NSA</b>	Necessary step to ensure accuracy
	<b>CET</b>	Correct error timely
	<b>VAI</b>	Verify accuracy of info
Improper Access	<b>EUA</b>	Efforts to Ensure Unauthorized
	<b>DPU</b>	Data protected from unauthorized
	<b>PUA</b>	Prevent unauthorized access
Unauthorized Secondary use	<b>NOP</b>	Use for no other purpose
	<b>NOU</b>	No other use
	<b>NSI</b>	Never sell EHR info.
	<b>NUS</b>	No unauthorized share of info

Table 4-6: Variables used in the four CFIP dimensions

$H_0$  = means of the three groups are the same mean (online) = mean (street) = mean (classroom)

$H_1$  = means are different.

Rejection of  $H_0$  is when P-Value is below 5.0% (i.e. p-value < 0.05)

	Online (on+)		Street (fd+)		Classroom		ANOVA RESULT				
Variables	Mean	Std Dev	Mean	Std Dev	Mean	Std Dev	SSC	SSE	F	P-Value	Conclusion
<b>BGI</b>	2.476	1.210	1.870	1.060	2.373	1.060	12.389	1.194	10.374	0.000	H <sub>0</sub> is rejected
<b>TTD</b>	2.988	1.310	2.678	1.210	3.032	1.210	5.092	1.573	3.237	0.042	H <sub>0</sub> is rejected
<b>BMI</b>	3.000	1.300	2.730	1.200	2.996	1.200	3.045	1.544	1.972	0.140	Failed to reject H <sub>0</sub>
<b>MIC</b>	2.929	1.190	2.670	1.180	2.992	1.180	4.155	1.395	2.978	0.052	Failed to reject H <sub>0</sub>
<b>ARC</b>	4.140	0.980	4.409	0.800	4.036	0.890	5.499	0.788	6.974	0.001	H <sub>0</sub> is rejected
<b>NSA</b>	4.593	0.790	4.652	0.590	4.652	0.590	1.712	0.503	3.388	0.035	H <sub>0</sub> is rejected
<b>CET</b>	4.756	0.590	4.652	0.530	4.472	0.710	3.077	0.415	7.413	0.001	H <sub>0</sub> is rejected
<b>VAI</b>	4.667	0.660	4.487	0.730	4.405	0.710	2.173	0.500	4.343	0.014	H <sub>0</sub> is rejected
<b>EUA</b>	4.791	0.560	4.678	0.540	4.516	0.790	2.788	0.476	5.856	0.003	H <sub>0</sub> is rejected
<b>DPU</b>	4.750	0.530	4.678	0.630	4.587	0.730	0.942	0.455	2.070	0.127	Failed to reject H <sub>0</sub>
<b>PUA</b>	4.807	0.570	4.791	0.540	4.655	0.620	1.143	0.351	3.258	0.040	H <sub>0</sub> is rejected
<b>NOP</b>	4.780	0.690	4.687	0.680	4.397	0.960	6.280	0.712	8.727	0.000	H <sub>0</sub> is rejected
<b>NOU</b>	4.872	0.500	4.765	0.580	4.631	0.740	2.092	0.442	4.733	0.009	H <sub>0</sub> is rejected
<b>NSI</b>	4.797	0.600	4.809	0.540	4.659	0.750	1.177	0.455	2.584	0.077	Failed to reject H <sub>0</sub>
<b>NUS</b>	4.762	0.650	4.748	0.53	4.587	0.74	1.546	0.460	3.361	0.036	H <sub>0</sub> is rejected

Table 4-7: ANOVA result indicated that the three samples could not be combined into one sample.

From Table 4-7, among the three groups (online, street and classroom) survey results, the ANOVA result of many variables are failed to reject H<sub>0</sub>. This suggests that the populations of the three groups are statistically different.

We further perform the ANOVA test on the online and street group to determine if the data from these two groups can be combined to form one group. We set out the hypothesis as follow:

**Null hypothesis H<sub>0</sub>** = means of the two groups are the same mean (online) = mean (street)

**Alternative hypothesis H<sub>1</sub>** = means are different. Rejection of H<sub>0</sub> is when P-Value is below 5.0% (i.e. p-value < 0.05)

	Online (on+)		Street (fd+)		ANOVA RESULT				
Variables	Mean	Std Dev	Mean	Std Dev	SSC	SSE	F	P-Value	Conclusion
<b>BGI</b>	2.476	1.210	1.870	1.060	18.140	1.279	14.184	0.000	<b>H0 is rejected</b>
<b>TTD</b>	2.988	1.310	2.678	1.210	4.732	1.719	2.753	0.099	Failed to reject H0
<b>BMI</b>	3.000	1.300	2.730	1.200	3.527	1.689	2.089	0.150	Failed to reject H0
<b>MIC</b>	2.929	1.190	2.670	1.180	2.888	1.399	2.064	0.152	Failed to reject H0
<b>ARC</b>	4.140	0.980	4.409	0.800	3.565	0.785	4.544	0.034	<b>H0 is rejected</b>
<b>NSA</b>	4.593	0.790	4.652	0.590	0.172	0.467	0.369	0.544	Failed to reject H0
<b>CET</b>	4.756	0.590	4.652	0.530	0.529	0.311	1.698	0.194	Failed to reject H0
<b>VAI</b>	4.667	0.660	4.487	0.730	1.568	0.494	3.171	0.077	Failed to reject H0
<b>EUA</b>	4.791	0.560	4.678	0.540	0.622	0.298	2.087	0.150	Failed to reject H0
<b>DPU</b>	4.750	0.530	4.678	0.630	0.250	0.35	0.715	0.127	Failed to reject H0
<b>PUA</b>	4.807	0.570	4.791	0.540	0.012	0.306	0.040	0.842	Failed to reject H0
<b>NOP</b>	4.780	0.690	4.687	0.680	0.418	0.470	0.888	0.347	Failed to reject H0
<b>NOU</b>	4.872	0.500	4.765	0.580	0.562	0.303	1.856	0.175	Failed to reject H0
<b>NSI</b>	4.797	0.600	4.809	0.540	0.006	0.322	0.019	0.892	Failed to reject H0
<b>NUS</b>	4.762	0.650	4.748	0.53	0.001	0.340	0.028	0.867	Failed to reject H0

Table 4-8: ANOVA result indicated that street and online samples could be combined

Table 4-8 shows the result of analysis of variance (ANOVA) with a convenience sample (classroom sample removed). The fitting is improved with  $H_0$  failed to reject. With the classroom sample being removed, there is a more frequent “failed to reject the  $H_0$ ” mean of Online and Street survey groups are the same mean.

#### 4.5 Overall Result of the Concern For Information Privacy (CFIP) Dimensions

This part of the chapter discusses the result of the survey data related to the four CFIP dimensions. Each dimension in the CFIP is composed of three or four survey variables. For example, the collection dimension is comprised of four survey variables. They are BGI, TTD, BMI, and MIC.



CFIP factor	Variable name	Description
<b>Collection (too much)</b>	<b>BGI</b>	Bothers me when I Give our private Information
	<b>TTD</b>	Think Twice before Disclosure
	<b>BMI</b>	Bothered Me when too much Information is collected
	<b>MIC</b>	Too much Information is Collected

Table 4-9: Meaning of variables in collection dimension.

To calculate the mean of the dimension, the mean of each variable within the dimension is first calculated. An overall mean is then calculated by finding the mean of all the means of the variable within the dimension. This overall mean is called the grand mean and it represents the mean of the dimension. In this case, the Grand Mean of the CFIP “collection” dimension is the mean of the BGI mean, TTD mean, BMI mean and MIC mean. A counter check of the value can also be verified by finding the average in the “Add” column in Table 4-10 below. The “Add” column is a summation of the four variables composed of the dimension in the CFIP model.

Q6	Q10	Q15	Q20		
<b>BGI</b>	<b>TTD</b>	<b>BMI</b>	<b>MIC</b>	<b>Add</b>	<b>Average</b>
2	2	3	3	11	2.75
2	3	2	2	9	2.25
5	5	0	0	10	2.50
1	1	2	1	5	1.25
3	4	3	3	13	3.25
1	1	1	1	4	1.00
1	1	1	1	4	1.00
Mean Value of the CFIP Collection dimension =					1.96

Table 4-10: Illustration of calculating the dimension means using “dummy” numbers

By using the method described in the illustration of calculating the mean of the dimension in Table 4-10 above, we calculated the following means of each dimension.

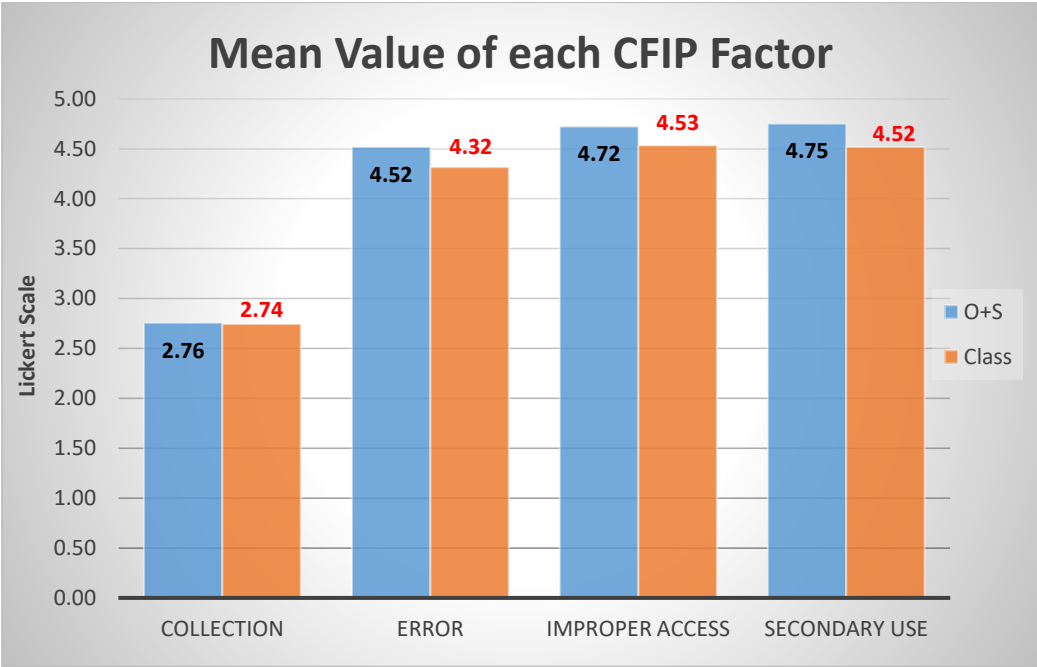


Figure 4-2: Overall survey result of the CFIP dimensions

**Observations**

Figure 4.2 above shows the “Online and Street (O+S)” survey sample that has a higher concern across three of the four dimensions than the classroom sample. The mean value of 2.76 from the collection [too much collection] dimension (between 2 = disagree and 3 = neutral or undecided) suggests that respondents (patients) have a lower level of concern (higher level of comfort) in terms of [too much collection] Collection dimension of health data from service providers. This is not surprising. This finding is consistent with a national survey done by Canadian Health Infoway in April 2012. Their findings from a sample of 2509 across Canada show that in general, Canadian patients trust their service providers (83% on doctors, 79% of pharmacists and 68% of nurses). Culturally, Canadian health-care providers especially the doctors and medical

specialists are well respected, and therefore they are bestowed with the trust of patients.

Of the other three dimensions (Error, Improper Access, and Secondary Use), the mean value for both the Online & Street survey (range from 4.52 to 4.75) and the classroom survey (ranges 4.32 to 4.53) indicated a higher degree of concern as compared to the “collection” dimension. A score of 4 = agree, and a score of 5 indicated strongly agree (to the questions that there are concerns of privacy in that particular dimension). A closer look at the three dimensions, the “Error”; the “Improper Access”; and the “Secondary Use” dimensions all yield a high mean score of 4.52, 4.72 and 4.75 respectively. This implies that the average attitude of respondents is in-between agree and strongly agree categories. This means that respondents have privacy concerns on these three CFIP dimensions: Errors in EHR information, Improper Access of EHR information and privacy concerns on Secondary Use of EHR information. The greatest privacy concern dimension is Unauthorized Secondary Use.

#### **4.5.1 DIMENSION 1: Privacy Concerns on Unauthorized Secondary Use of Information**

Secondary use of information includes the use of EHR data in research, government administrative functions and the use for public health management that are not aware by the patient and therefore received no authorization from the patient. This is different from the primary use of the information to heal the illness of the patient.

To assess the patient's concern about secondary use, four questions were included in the survey. They were:

Categories of Concern	Variable	Description
Secondary use	NOP	Use for no other purpose
	NOU	No other unrelated reasons
	NSI	Never sell EHR info.
	NUS	No Unauthorized sharing of info

Table 4-11: Meaning of variables in CFIP secondary use.

#### (A) No Other Purpose (NOP)

Variable	Description					
NOP	Service providers should not use personal health information for any purpose unless it has been authorized by the individual who provided the information.					
NOP	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	Values below are in % of total respondents					
Sample 1: Online+ Street Survey (%)	0.5	3.0	1.5	13.4	81.6	201
Sample 2: Classroom Survey (%)	2.4	4.4	6.3	25.0	61.9	252

Table 4-12: Result of the 5-point Likert scale on NOP secondary use.

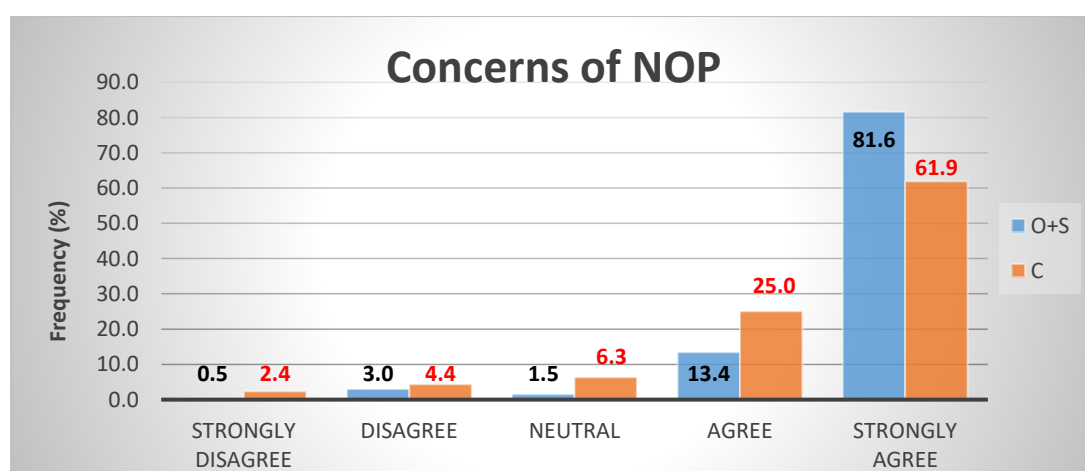


Figure 4-3: Percent Frequency for NOP

**Online & Street (O+S) survey group: (201 respondents)**

From the responses as presented in the above Table 4-12, 95% (13.4%+81.6%) which translated to 190 out of total 201 of respondents agree or strongly agree that service providers should not use personal health information for any purpose unless they have been authorized to do so by the individual who provided the information. This is in contrast to only 3.5% (7 out of a total 201) of respondents who disagree. Only 1.5% (3 out of a total 201) respondents are neutral or undecided on this question.

**For classroom survey group: (252 respondents)**

From the responses as presented in the above Table 4-12, 87.0% (219 out of total 252 respondents) of responses agrees or strongly agrees that service providers should not use personal health information for any purpose unless it has been authorized by the individual who provided the information. This is in contrast to 6.8% (17) respondents who disagree. There are 6.3% (16) of respondents express a neutral position to this question.

**Observations**

When adding the agree and strongly agree categories in Figure 4-3, the online and street survey group has a higher (8.1% = 95% - 86.5%) than the classroom survey group in concurrence regarding the concerns of Secondary Use of data. The EHR data must not be used for other purpose unless it has been authorized by the patient who provided the information.

The online and street survey group has clearly indicated a strong attitude (81.6% strongly agree) that the Secondary Use of information should be for no other purpose except to aid the treatment of patients in contrast to a 61.9% in the classroom survey group.

A different pattern appeared in the strongly disagree + disagree categories. The classroom survey group seems to be less concern (6.8% vs. 3.5%) when compared with the online and street survey group.

**(B) No Other Unrelated Reasons (NOU)**

Variable	Description					
NOU	Service providers should not use personal health information for any purpose unless this has been authorized by the individual who provided the information.					
NOU	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Online and Street Survey (%)	0.5	1.0	1.5	10.9	86.1	201
Classroom Survey (%)	1.0	1.0	1.5	10.9	85.6	252

Table 4-13: Result of the 5-point Likert scale on NOU secondary use.

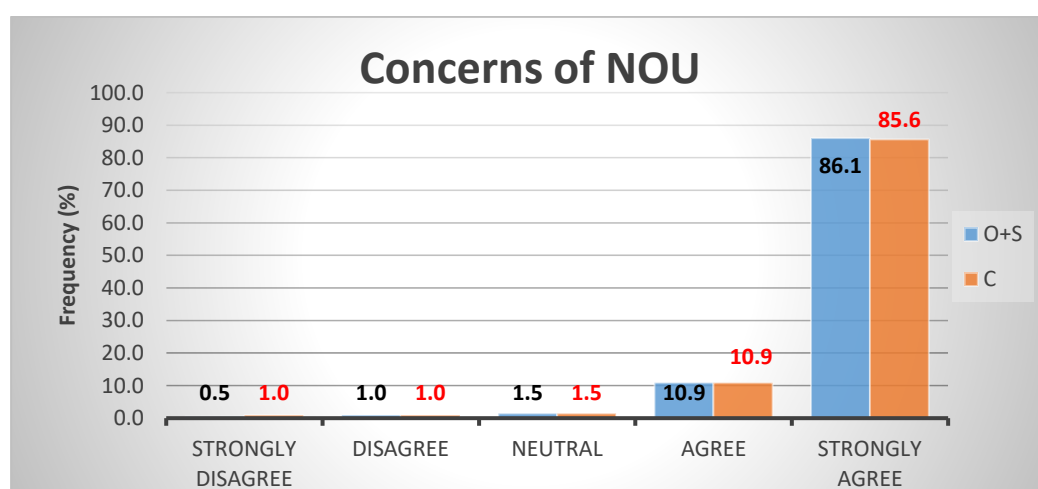


Figure 4-4: Percent Frequency for NOU.

**Online & street survey group: (201 respondents)**

From the responses as presented in the above Table 4-13, 97% (195 out of total 201) of respondents agree or strongly agree that service provider should not use the information for other unrelated reasons, especially for commercial benefits. This is in contrast to only 1.5% (3 out of a total 201) of respondents who

disagree. 1.5% (3 out of a total 201) of respondents were neutral to this question.

### **Classroom survey group: (252 respondents)**

From the responses as presented in the above Table 4-13, 96.5% (243 out of total 252) of respondents agree or strongly agree that service provider should not use the information for other unrelated reasons, especially for commercial benefits. This is in contrast to 2.0% (5) of respondents who disagree. 2.0% (5) of respondents who have expressed a neutral position to this question.

### **Observations**

From both the online and street survey group and classroom survey groups, there is a high percentage, about 97% of the respondents, who have disapproved and clearly indicated that service provider should not use their personal health information for other unrelated reasons, especially for commercial benefits.

### **(C) Never Sell Information (NSI)**

Variable	Description					
NSI	Service providers should never sell the EHR personal information to other organizations					
NSI	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents.
	% of total respondents					
Sample 1: Online+ Street Survey (%)	0.5	1.0	2.0	10.6	85.9	199
Sample 2: Classroom Survey (%)	2.0	1.0	2.0	10.4	84.7	202

Table 4-14: Result of the 5-point Likert scale on NSI secondary use.

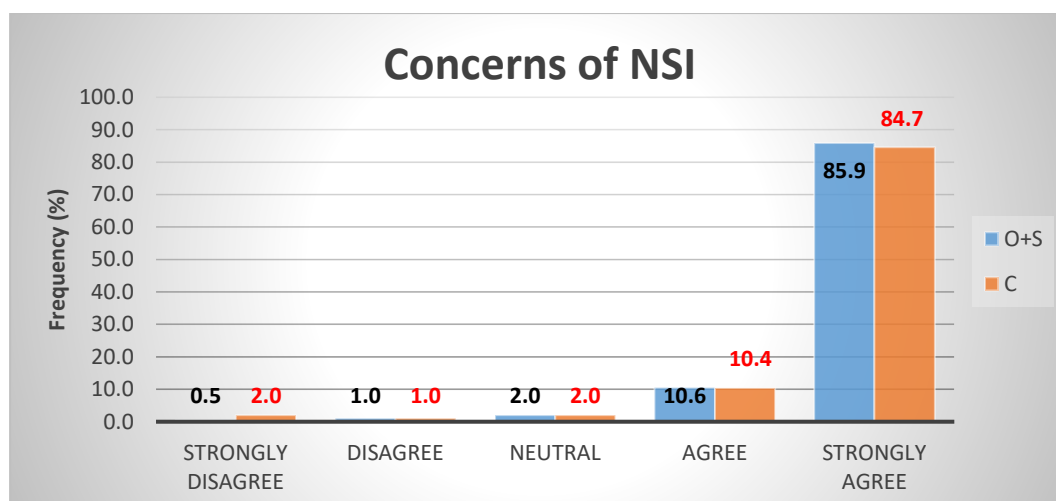


Figure 4-5: Percent Frequency for NSI.

### **Online & street survey group: (199 respondents)**

From the responses as presented in the above Table 4-14, 96.5% (192 out of total 199) of respondents agree or strongly agree that service providers should never sell the EHR personal information to other organizations. This is in contrast to only 1.5% (3 out of a total of 199) respondents who disagree. There are 2.0% (4 out of 199) of respondents expressed neutral position to this question.

### **Classroom survey group: (202 respondents)**

From the responses as presented in the above Table 4-14, 95.1% (192 out of 202) of respondents agree or strongly agree that Service providers should never sell the EHR personal information to other organizations. This is in contrast to 1.2% of respondents who disagree. There are 2.9% of respondents strongly disagreed with this statement. There are 2.0% of respondents expressed a neutral position to this statement.

### **Observations**

Both the online and street survey group and the classroom group yields very high and similar (85%, 86% respectively) agreement that service providers should never sell the EHR personal information to other organizations. There is a high concordance between the online & street survey group and the classroom group across all the Likert item except in the strongly disagree



category. It is of interest to observe that even a question of selling the EHR personal information that generally would be considered unethical and may infringe on the privacy law in Ontario, there are still some 2% (4 out of 202) respondents expressed strongly disagree in the classroom survey group. It suggested that a small number of respondents have no concerns at all if service provider were to sell their personal health information to other organization.

**(D) No Unauthorized Sharing (NUS)**

Variable	Description					
NUS	Service providers should not share personal health information with other companies unless it has been authorized by the individual who has provided the information.					
NUS	Strongly Disagree	Disagree	Neutr al	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Sample 1: Online+ Street Survey (%)	0.5	1.0	1.5	16.6	80.4	199
Sample 2: Classroom Survey (%)	2.0	1.0	1.5	16.3	79.2	202

Table 4-15: Result of the 5-point Likert scale on NUS secondary use.

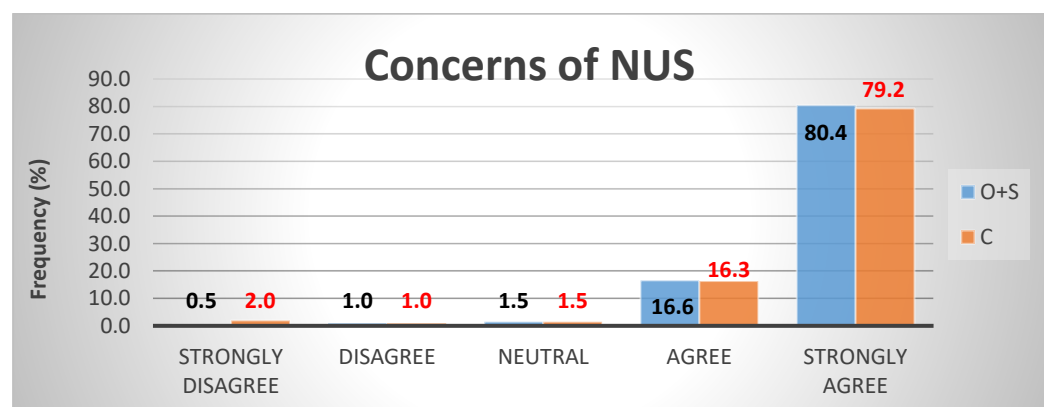


Figure 4-6: Percent Frequency for NUS.

**For online & street survey group: (199 respondents)**

From the responses as presented in the above Table 4-15, 97% (193 out of total 199) of respondents agree or strongly agree that service providers should never sell the EHR personal information to other organizations. This is in contrast to only 1.5% (3 out of a total 199 respondents) who disagrees. There are 1.5% (3 out of 199) participants who expressed a neutral position to this question.

**For classroom survey group: (202 respondents)**

From the responses as presented in the above, Table 4-15, 95.5% (193 out of total 202) of those surveyed) agree or strongly agree that Service providers should never sell the EHR personal information to other organizations. This is in contrast to 3% (6) of respondents who disagree. Only 1.5% (3) of respondents expressed a neutral position to this question.

**Observations**

There is a very high percentage on both the online and street survey group (80.4% and 79.2%, respectively) feel strongly agree that there should be no unauthorized sharing of information provided. There is a similar pattern to the NSI (Never sell EHR information) and NOU (No Other Unrelated reasons) questions for which the online group has a slightly higher strongly agree, and a similar percentage result on the agree responses compared to the street survey group.

**4.5.2 DIMENSION 2: Privacy Concerns on Improper Access**

The second CFIP dimension is Improper Access. This dimension concerned with unauthorized persons having access to the information. When unauthorized access takes place, the planned system security; defense mechanisms and controls will not be alerted. This means the function of controls in the prevention, detection, and correction procedure will be bypassed.

The improper access dimension is riskier than the other two CFIP dimensions such as “Errors and Secondary use.” Although the error in EHR can be dangerous in assisting the treatment, it does not necessarily result in privacy

exposure. Privacy exposure is the main construct of our research question. For secondary use of EHR data, such as for research purposes and public health management there are set protocols that must be adhered to before summarized data can be given to researcher. Three variables were used in the survey to investigate the privacy concerns of the CFIP dimension: improper access dimension.

Categories of Concern	Variable	Description
Improper Access	<b>EUA</b>	Efforts to prevent Unauthorized Access
	<b>DPU</b>	Data Protected from Unauthorized access
	<b>PUA</b>	Prevent Unauthorized Access

Table 4-16: Meaning of variables in CFIP Improper access.

**(A) Efforts to Prevent Unauthorized Access (EUA)**

Variable	Description					
EUA	Service providers should devote the necessary time and effort to preventing unauthorized access to personal information.					
EUA	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Online+ Street Survey (%)	0.5	0.5	0.5	22.9	75.6	201
Classroom Survey: (%)	1.2	1.6	6.3	26.2	64.7	252

Table 4-17: Result of the 5-point Likert scale on EUA in improper access.

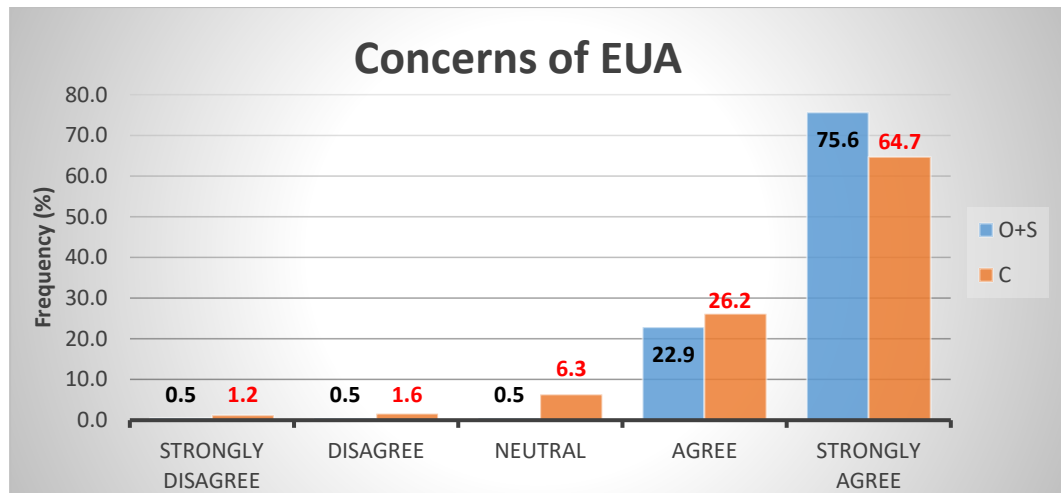


Figure 4-7: Percent Frequency for EUA

### Online and street survey group: (201 respondents)

From the responses presented in the above Table 4-17, 98.5% (198 out of a total 201) of respondents agree or strongly agree that service providers should devote the necessary time and effort to preventing unauthorized access to personal information. Their attitude is that service providers should ensure efforts in preventing unauthorized access to personal information provided by the patients. There is a concern towards the unauthorized access of EHR entrusted with service providers. This is in contrast to 1.0% (2 out of a total 201) respondent who strongly disagrees (feeling comfortable) that they have no concern about the ways that EHR data were collected. There is one participant in a neutral/undecided position.

### Classroom survey (252 respondents)

From the responses presented in the above Table 4-17, there is 90.9% (229 out of total 252) of the respondents agree or strongly agree that service providers should devote the necessary time and effort to preventing unauthorized access to personal information. This is in contrast to 2.87% (7) of the respondents disagreeing that service providers should devote the necessary time and effort to preventing unauthorized access to personal information. 6.3% (13) of the respondents expressed a neutral position in this question.

## Observations

Overwhelmingly, 98.5% in Online and Street survey and 90.9% of Classroom respondents view the unauthorized access of their private information as a critical issue. They expect service providers to devote the necessary time and effort to keep their data safe and away from unauthorized access. Very few (less than 3%) respondents in either group feel comfortable with service provider's effort in preventing unauthorized access to their personal information.

### (B) Databases Protected from Unauthorized access (DPU)

Variable	Description					
DPU	Computer databases that contain my personal health information should be protected from unauthorized access, regardless of cost.					
DPU	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Online+ Street Survey (%)	0.0	1.0	4.0	18.1	76.9	199
Classroom Survey: (%)	0.5	1.0	4.0	18.0	76.5	200

Table 4-18: Result of the 5-point Likert scale on DPU in improper access.

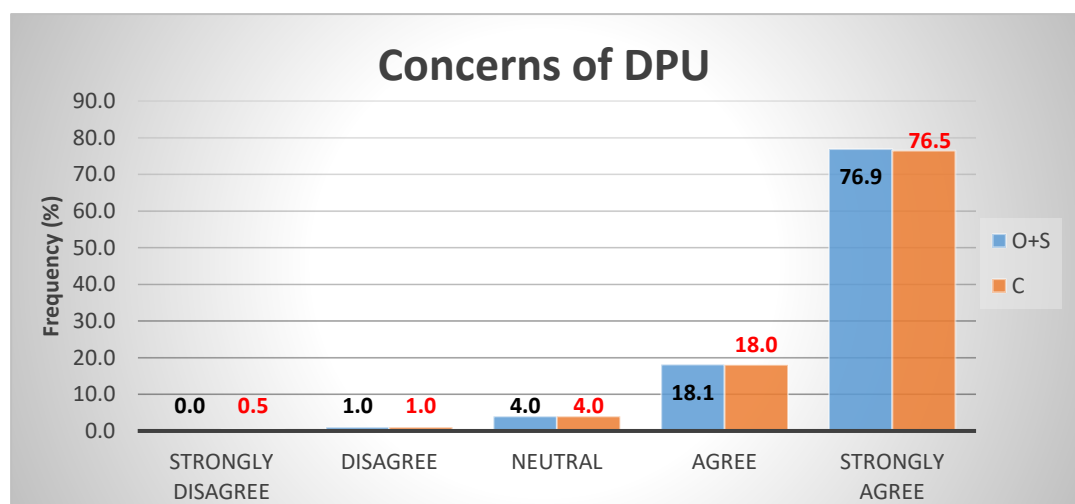


Figure 4-8: Percent Frequency for DPU.

**Online & Street Survey group: (199 respondents)**

From the responses as presented in the above Table 4-18, 95% (189 out of total 199) of respondents agree or strongly agree that computer databases that contain their personal health information with their service provider should be protected from unauthorized access, regardless of cost. This is in contrast to 1% (2 out of a total 199) respondents who disagree that computer databases that contain their personal health information with service providers should be protected from unauthorized access, regardless of cost. 4.0% (8 out of a total of 199) respondents who are neutral or undecided on this question.

**Classroom survey: (200 respondents)**

From the responses as presented in the above Table 4-18, 94.5% (189 out of total 200) of respondents agree or strongly agree that computer databases that are containing their personal health information with their service provider should be protected from unauthorized access, regardless of cost. This is in contrast to 1.5% (3) of respondents who disagree that computer databases that are containing their personal health information with their service provider should be protected from unauthorized access, regardless of cost. 4.0% (8) of respondents who have expressed a neutral or undecided position to this question. Only 1.0% from online and street survey group and 1.5% from classroom survey group disagree with the requirement of protection from the service provider of their databases regardless of cost.

**Observations**

The online and street survey group has a 95.0%, and classroom survey group has a 94.5% of respondents respectively have the attitude that unauthorized access of their private information is a critical issue. They expect the service provider to protect their private data in the provider database regardless of cost. In sharp contrast, that there is only 1.0% from online and street survey group and 1.5% from classroom survey group that disagree with the requirement of protection from the service provider on their databases regardless of cost.

(C) Protection of Unauthorized Access (PUA)

Variable	Description					
PUA	Service providers should take necessary steps to ensure that unauthorized people cannot access personal information in their EHR system					
PUA	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Online & Street Survey (%)	1.0	0.0	1.0	14.1	83.8	198
Classroom Survey: (%)	0.5	0.0	1.0	14.2	84.3	197

Table 4-19: Result of the 5-point Likert scale on PUA improper access.

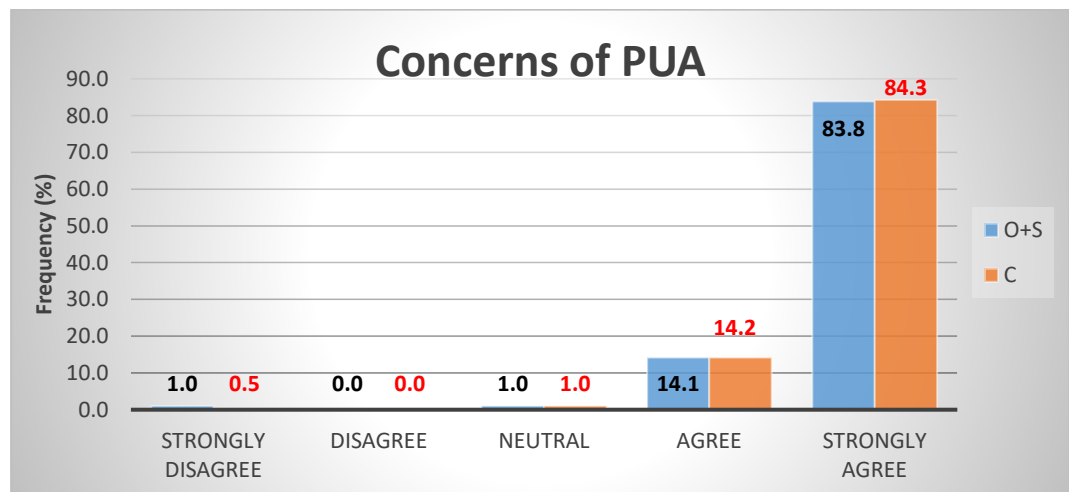


Figure 4-9: Percent Frequency for PUA

**Online & street survey group: (198 respondents)**

From the responses as presented in the above Table 4-19, 97.9% (194 out of a total 198) respondents agree or strongly agree service providers should take necessary steps to ensure that unauthorized people cannot access personal information in their EHR system. This is in contrast to 1.0% (2 out of a total 198) respondents who strongly disagree (are comfortable) that service providers should take necessary steps to ensure that unauthorized people cannot access

personal information in their EHR system for the neutral category. Only 1.0% (2 out of a total 198) of respondents are neutral or undecided on this question.

**For classroom survey group: (197 respondents)**

From the responses as presented in the above Table 4-19, 98.5% (194 out of a total 197) of respondents agree or strongly agree that service providers should take necessary steps to ensure that unauthorized people cannot access personal information in their EHR system. This is in contrast to 0.5% (1 out of a total 197 respondents) of respondents that strongly disagree that service providers should take necessary steps to ensure that unauthorized people cannot access personal information in their EHR system. Only 1.0% (2 out of a total 197) of respondents expressed a neutral position in this question.

**Observations**

Overwhelmingly, both online and street survey and classroom survey groups have a very high privacy concern on the service provider and expect that service provider should take necessary step to ensure that unauthorized people cannot access personal information in their EHR system.

This question of PUA (Prevent Unauthorized Access) is a complementary follow-up question with the DPU (Data Protected from Unauthorized access) question. The responses to both questions yield a highly similar frequency distribution suggesting that the validity of DPU (Q14) is confirmed with PUA (Q19).

### **4.5.3 DIMENSION 3: Privacy Concerns of Information Errors**

The fourth important CFIP dimension is regarding Errors on the EHR. Although the error in EHR can be dangerous in assisting the treatment of patients, it does not necessarily result in privacy exposure. Privacy exposure is the main construct of our research question. For this reason, the error of EHR record could be an operational or human error, but not necessarily a privacy concern. There are error protocols, validity and integrity check normally built-in for a database.



Categories of Concern	Variable	Description
Error in records	ARC	Accuracy regardless of cost
	NSA	Necessary step to ensure accuracy
	CET	Correct error timely
	VAI	Verify accuracy of info

Table 4-20: Meaning of variables in CFIP error.

### (A) Accuracy Regardless of Cost (ARC)

Variable	Description					
ARC:	All the personal health information in computer databases should be double-checked for accuracy, regardless of costs					
ARC	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Sample 1: Online + Street Survey (%)	1.5	4.0	8.5	36.0	50.0	200
Sample 2: Classroom Survey: (%)	2.0	4.4	12.7	50.0	31.0	252

Table 4-21: Result of the 5-point Likert scale on ARC error of information.

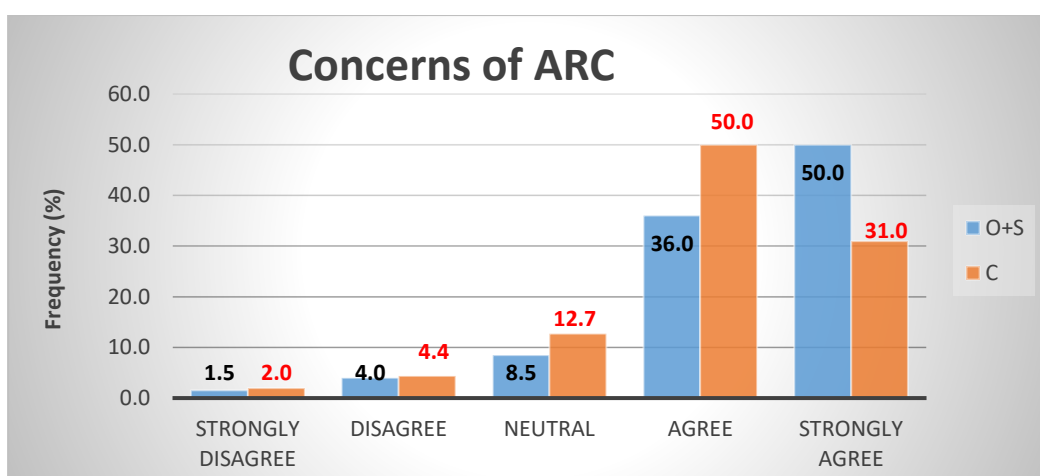


Figure 4-10: Frequency in percentage for ARC

**Online & street survey group: (200 respondents)**

From the responses as presented in the above Table 4-21, 86% (172 out of total 200) of respondents agree or strongly agree that all personal health information in computer databases in the service provider should be double-checked for accuracy, regardless of costs. This is in contrast to 5.5% (11 out of a total 200 respondents) who disagree. There are 8.5% (17 out of 200) of respondents in the neutral position to this question, suggesting less certainty regarding accuracy as compared to privacy.

**Classroom survey group: (252 respondents)**

From the responses as presented in the above Table 4-21, 81.0% (204 out of total 252) respondents agree or strongly agree that all the personal health information in computer databases in the service provider should be double-checked for accuracy, regardless of costs. This is in contrast to 6.4% (16 participants) who disagree. There is a sizable group of 12.7% (32) of respondents expressed a neutral position to this question.

**Observations**

Regarding ARC (Accuracy regardless of cost), both the online and street survey group and the classroom survey group yield a similar result as 86.0% and 81.0% respectively on the strongly agree and agree categories. However, in the strongly agree category, there is a sizable difference between the percentages of the two groups with online & street survey group were 19.0% higher than the classroom group. A reverse outcome happened in the agree categories.

This is a similar result when adding up the strongly agree and agree responses. There is not much difference observed between the percentages of respondents agreeing or strongly agreeing whether they came from online and street survey group or classroom group. There is a majority of respondents expressing concerns of errors in their patient's records and that they expect the service provider to double-check the database information regardless of cost. With the understanding that databases already have some forms of error detection, respondents are suggesting that the responsibility still lies with the service providers who collect the information and input it into the database. In this

ARC question, we observe that more respondents are selecting the neutral position on both online and street survey group than the classroom group.

**(B) Necessary Steps for Accuracy (NSA)**

Variable	Description					
NSA:	Service providers should take necessary and appropriate steps to make sure that the personal health information in their files is accurate					
NSA	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Sample 1: Online+ Street Survey (%)	1.0	1.0	2.5	25.4	70.1	201
Sample 2: Classroom Survey (%)	1.2	0.4	6.0	36.5	56.0	252

Table 4-22: Result of the 5-point Likert scale on NSA error of information.

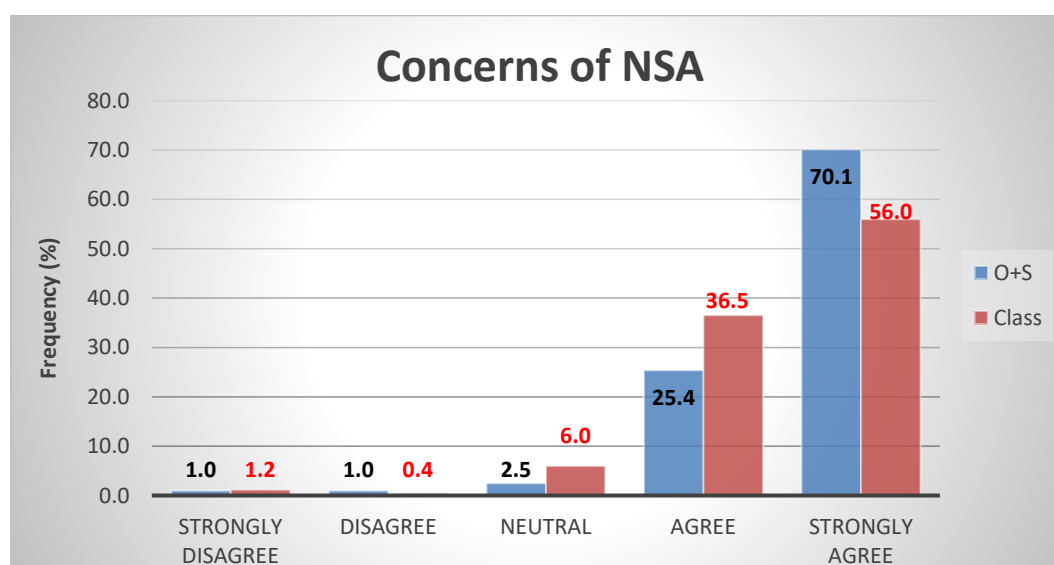


Figure 4-11: Percent Frequency for NSA.

**For online and street survey group: (201 respondents)**

From the responses as presented in the above Table 4-22, 95.4% (192 out of total 201 respondents) agree or strongly agree that service providers should take necessary and appropriate steps to make sure that the personal health information in their files is accurate. This is in contrast to only 2% (4

respondents) who disagree. There are 2.5% (5) respondents in the neutral position to this question.

**For classroom survey group: (252 respondents)**

From the responses as presented in the above Table 4-22, 92.5% (233 out of total 252) respondents agree or strongly agree that service provider should take necessary and appropriate steps to make sure that the personal health information in their files is accurate. This is in contrast to 1.6% (4 participants) of respondents who disagree. There are 5.9% (15) of respondents expressed neutral to this question.

**Observations**

Regarding the question of NSA (Necessary step to ensure accuracy), respondents in both online and street survey and classroom survey group are comparable in both the strongly agree and agree responses (95.5% vs. 92.5%). Regarding the neutral responses, there is a lower number of responses 2.5% from online & street survey group than the 5.9% from classroom survey group. In this variable NSA than the previous variable of ARC (database should be checked for Accuracy regardless of Cost).

**(C) Correct Errors Timely (CET)**

Variable	Description					
CET	Service providers should have procedures in place to correct errors in EHR information in a timely manner.					
CET	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Sample 1: Online+ Street Survey (%)	0.5	0.0	2.0	24.4	73.1	201
Sample 2: Classroom Survey (%)	0.4	0.8	7.5	33.7	57.5	252

Table 4-23: Result of the 5-point Likert scale on CET error of information.

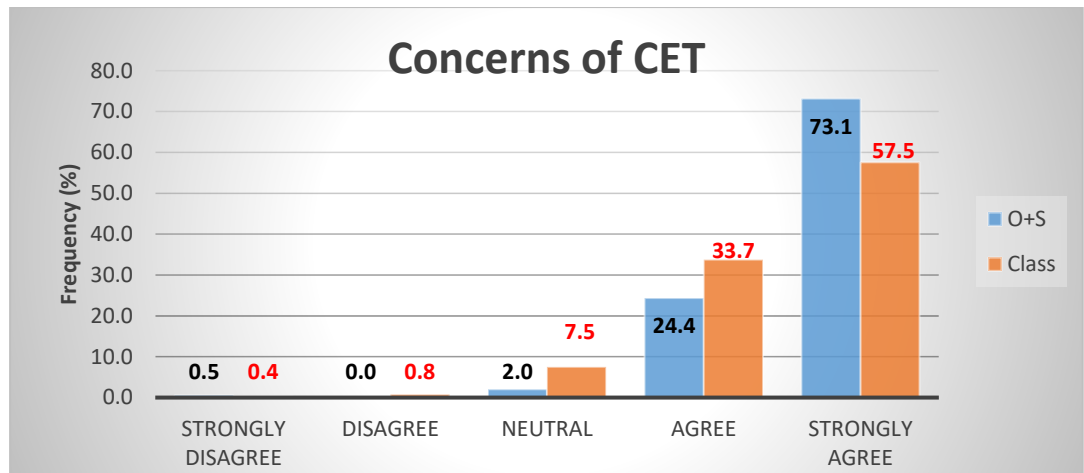


Figure 4-12: Percent Frequency for CET.

### **Online & street survey group: (201 respondents)**

From the responses as presented in the above Table 4-23, 97.5% (196 out of total 201 respondents) strongly agree or agree that service providers should have procedures in place to correct errors in EHR information in a timely manner. This is in contrast to only 0.5% (1 participant) who disagrees. There are also 2.0% (4) respondents in the neutral position to this question.

### **Classroom survey group: (252 respondents)**

From the responses as presented in the above Table 4-23, 91.2% (230 out of total 252 respondents) strongly agree or agree that service providers should have procedures in place to correct errors in EHR information in a timely manner. This is in contrast to 1.2% (3 respondents) who strongly disagree or disagree. In addition, 7.5% (19 respondents) expressed a neutral position to this question.

### **Observations**

Regarding the question of CET (Correct error timely), there is apparently a very high expectation - agree and strongly agree categories (95.5%) from online & street survey respondents that service providers should have procedures in place to correct errors in EHR information in a timely manner. The online and street survey respondents have a 73.1% and in contrast the classroom survey respondents have a 57.5% in the strongly agree category which is significantly different from the online & street survey group.

**(D) Verify Accuracy of Information (VAI)**

Variable	Description					
VAI	Service providers should devote the necessary resources including time and effort towards verifying the accuracy of the personal health information in their databases.					
VAI	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Online+ Street Survey (%)	1.0	1.0	3.5	29.6	64.8	199
Classroom Survey (%)	0.8	0.8	6.0	42.1	50.4	252

Table 4-24: Result of the 5-point Likert scale on VAI error of information.

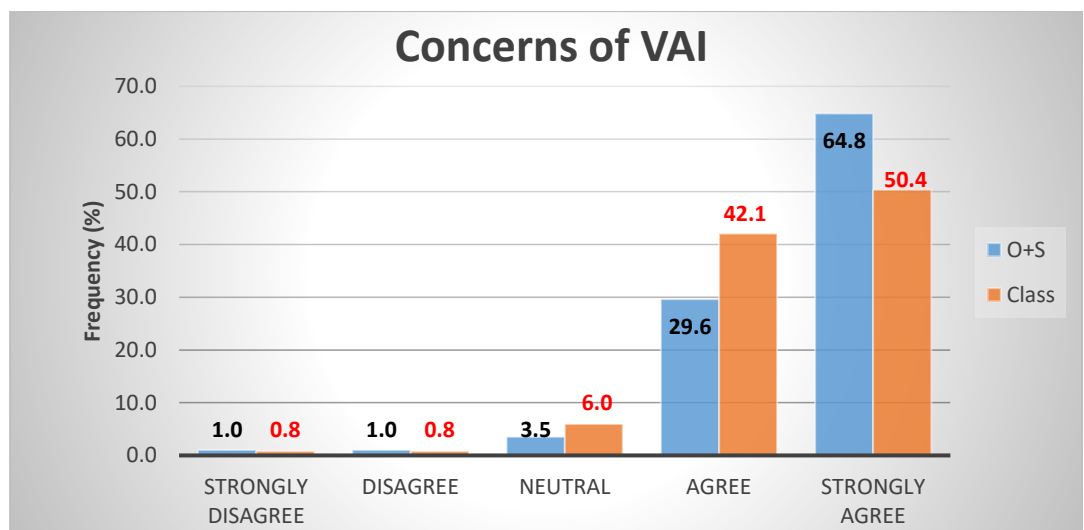


Figure 4-13: Frequency in percentage for VAI

**Online and street survey group: (199 respondents)**

From the responses as presented in the above Table 4-24, 94.4% (188 out of total 199 respondents) strongly agree or agree that service provider should devote the necessary resources including time and effort towards verifying the accuracy of the personal health information in their databases. This is in contrast to only 2.0% (4 out of a total 199 respondents) who disagree. Only 3.5% (7) respondents expressed a neutral position to this question.

**For classroom survey group: (252 respondents)**

From the responses as presented in the above Table 4-24, 92.5% (233 out of total 252) respondents agree or strongly agree that service providers should devote the necessary resources including time and effort towards verifying the accuracy of the personal health information in their databases. This is in contrast to 1.6% (4 respondents) who disagree. However, there are 5.9% (15) respondents expressed a neutral position to this question.

**Observations**

This variable VAI (Verify Accuracy of Information in the database) is used as a confirmatory variable to ARC (database should be checked for Accuracy Regardless of Cost) and NSA (Necessary Steps to ensure Accuracy) variables that were asked earlier in the survey. One of the validity checks used in this variable is to confirm the integrity of respondents' attitude that they did not change their overall response when similar questions were asked. The answers to these three variables yield very similar patterns with high portions of respondents indicating strongly agree and agree to the questions. When comparing to the CET (Correct Error Timely) variable, the patterns are also very similar, giving an overall pattern of information error responses in the Strongly agree and Agree categories. At the same time, there is a very low proportion in strongly disagree and disagree responses.

#### 4.5.4 DIMENSION 4: Privacy Concerns on Too Much Collection

Four variables were used in the survey to investigate the privacy concerns of the collection dimension.

CFIP dimension	Variable name	Description
<b>Collection (too much)</b>	<b>BGI</b>	Bothers me when I give info
	<b>BMI</b>	Bothers me when too much Information is collected
	<b>MIC</b>	Too much info. is collected
	<b>TTD</b>	Think twice before disclosure

Table 4-25: Meaning of variables in collection dimension.

#### (A) Bothers Me When Asked for Personal Health Information (BGI)

Variable	Survey Question					
BGI	It usually bothers me when health service providers ask me for personal health information					
BGI:	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Sample 1: Online + Street Survey (%)	37.3	32.8	13.9	11.4	4.5	201
Sample 2: Classroom Survey (%)	21.0	41.3	19.8	15.1	2.8	252

Table 4-26: Result of the 5-point Likert scale on BGI in the collection.



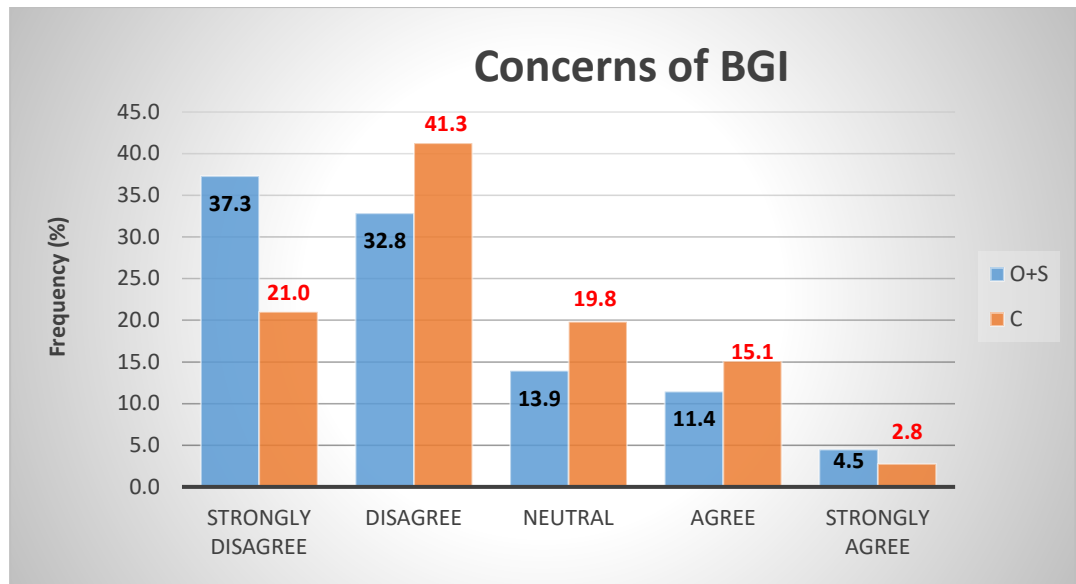


Figure 4-14: Percent Frequency for BGI

#### Online and Street survey group (201 respondents)

From the responses above in Table 4-26, 15.9% (32 out of 201) respondents agree or strongly agree that there is a concern (uncomfortable feeling) towards the collection of health data. This is in contrast to 70.1% of the same group of respondents disagree or strongly disagree (feeling comfortable) and that they have no concern about the ways that health and personal data are collected. It is important to note that 13.9% of the respondents are undecided or neutral on whether they have a concern on the collection of EHR data.

#### Classroom survey (252 respondents)

From the responses above in Table 4-26, 17.9% (45 out of a total 252) of respondents agree or strongly agree that there is a concern (uncomfortable feeling) towards the collection of private information. 62.3% (157) of respondents disagree or strongly disagree cumulatively (feeling comfortable) that they have no concerns about the ways that EHR data were collected. It is important to note that 19.8% (50) respondents are undecided on whether they have a concern on the collection of EHR data.

## Observations

It appears that more respondents (70.1%) from Online and Street Survey were more comfortable when service provider asked them for personal information than that of the Classroom survey (62.3%) respondents. This difference could be related to an older age of the Online & Street survey group.

The Online and Street Survey respondents have a declining trend among all categories from the highest percentage of strongly disagree to lowest percentage in strongly agree. This is in contrast to the Classroom Survey where there are fewer respondents in the strongly disagree than the disagree category. The Classroom Survey respondents are noticeably younger in age.

The survey results suggest that Ontario patients have a higher percentage of less concern (comfortable) regarding a collection of health data from service providers.

### (B) It Bothers Me to Give So Much Information (BMI)

Variable	Survey Question					
BMI	It bothers me to give so much personal information to service providers.					
BMI	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Sample 1: Online+ Street Survey (%)	18.6	25.6	20.6	23.1	12.1	199
Sample 2: Classroom Survey: (%)	13.8	27.1	21.8	24.5	12.8	188

Table 4-27: Result of the 5-point Likert scale on BMI in the collection.

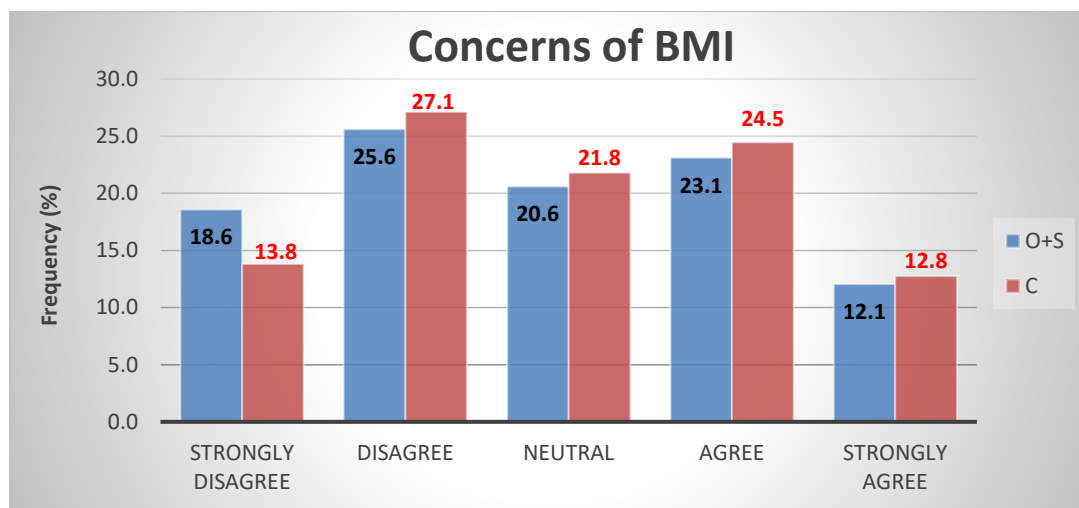


Figure 4-15: Percent Frequency for BMI.

### **The result from Online & Street survey group (199 participants)**

From the responses above in Table 4-27, 35.2% (70 out of total 199 respondents) of respondents agree or strongly agree that it bothers them to give so much personal information to service providers. There is a concern towards the collection of medical data. This is in contrast to 44.2% (88) of respondents who disagree or strongly disagree (feeling comfortable) that they have no concern and it does not bother them to give so much personal information to service providers on the ways that EHR data were collected. It is important to note that 20.6% (41) of respondents are undecided or neutral on whether they have privacy concern on a collection of EHR data.

### **The result from Classroom survey (188 respondents)**

From the responses above in Table 4-27, 37.3% (70 out of a total 188 respondents) of respondents agree or strongly agree that there is a concern (uncomfortable feeling) towards the collection of private personal and health information. This is in contrast to 40.9% (77 out of 188) of respondents who cumulatively disagree or strongly disagree (feeling comfortable) that they have no concern about the ways that EHR data were collected. It is important to note that 21.8% (41 out of 188) of respondents are undecided on whether they have a concern about a collection of EHR data.

## Observations

The classroom survey has a similar percentage of respondents feeling comfortable with service provider asking them for private information as in the online and street survey. It is also observed that there is a similar percentage 21.8% classroom vs. 20.6% in the online and street survey group are neutral in whether they are comfortable or uncomfortable when service providers ask for their personal information. It is also observed that in the strongly disagree Likert item, classroom participants are less concerned (4.8%) to give out much information when comparing that with the online and street survey group.

### (C) Too Much Information is Collected (MIC)

This variable is an alternative question validating the BMI variable.

Variable	Survey Question					
MIC	I am concerned that service providers are collecting too much personal health information about me.					
MIC	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Sample 1: Online+ Street Survey (%)	15.6	28.6	26.6	20.6	8.5	199
Sample 2: Classroom Survey: (%)	13.0	29.5	27.5	21.2	8.8	193

Table 4-28: Result of the 5-point Likert scale on the MIC in the collection.

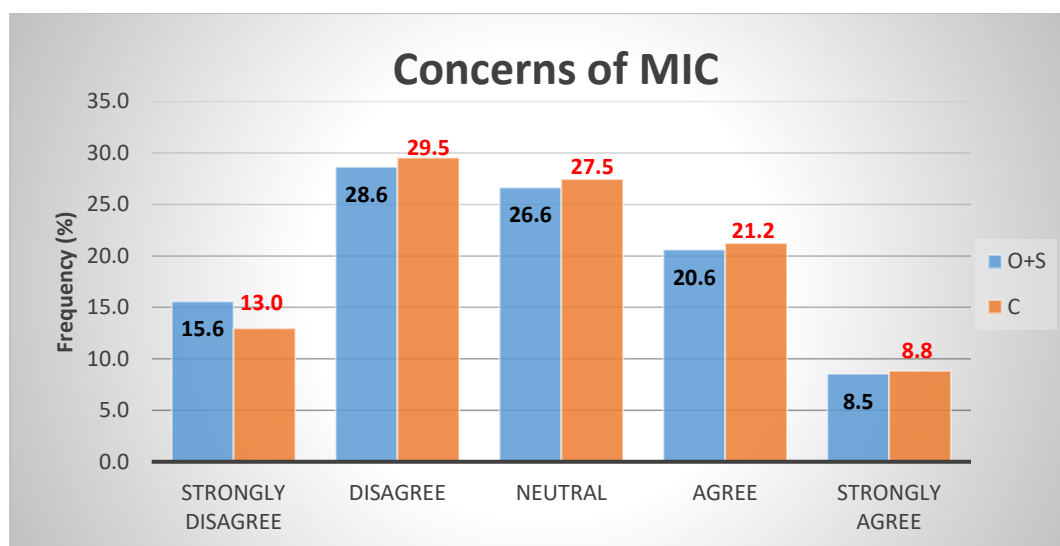


Figure 4-16: Percent Frequency for MIC.

### Online & Street survey group: (199 respondents)

From the responses above in Table 4-28, 29.1% (58 out of 199) of responses agree or strongly agree that service providers are collecting too much personal health information about me. In contrast, 44.2% (88) of respondents who disagree or strongly disagree cumulatively (feeling comfortable) that they have no concern about the ways that EHR data were collected. It is important to note that about one-quarter (53) of the 199 respondents are either neutral or undecided on whether they have a concern on a collection of EHR data.

### Classroom survey (193 respondents)

From the responses above in Table 4-28, 30.0% (58 out of a total 193) of respondents agree or strongly agree that service providers are collecting too much personal health information about them. There is a concern (uncomfortable feeling) towards the collection of EHR data. This is in contrast to 42.5% (82) respondents who disagree or strongly disagrees that service providers are collecting too much personal health information about them. They have no concern about the ways that EHR data were collected. It is important to note that 27.5% (53 respondents) is undecided on whether they have a concern about the collection of EHR data.

## Observations

The Classroom Survey group has a higher percentage of a comfort level than that of the online and street survey group regarding their attitude toward service provider collecting too much information about them. However, the online and street survey group has expressed fewer concerns (disagree or strongly disagree) with the question that service provider is collecting too much information than that of the online group. There are slightly more respondents who felt uncertain or neutral in the classroom survey respondents (28.7%) than that of the online and street respondents (23.8%).

When comparing the validity question MIC (Too much Information Collected) to the BGI (Bothers me when I give info) question, the two variables (BGI, MIC) yield a similar pattern of percentage responses in all categories.

Respondents who have answered BMI (Bothers me when too much Information is collected) earlier in the questionnaire have scored similar pattern across the strongly disagree to strongly agree category. This validity check confirms the trends of the higher number of disagreement to the Concerns for Information Privacy (CFIP) framework in the area of concern in the collection of EHR data.

### (D) Think Twice Before Disclosure (TTD)

Variable	Survey Question					
TTD	When service providers ask me for personal health information, I sometimes think twice before providing it.					
TTD	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total no. of respondents
	% of total respondents					
Sample 1: Online+ Street Survey (%)	19.5	29.5	12.0	29.5	9.5	200
Sample 2: Classroom Survey: (%)	14.8	31.2	12.7	31.2	10.1	189

Table 4-29: Result of the 5-point Likert scale on TTD in the collection.

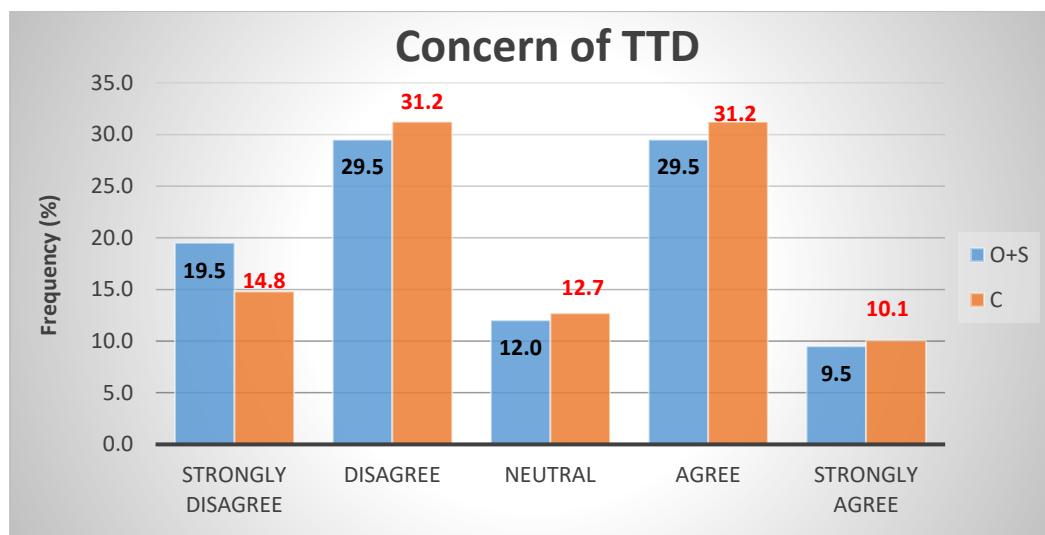


Figure 4-17: Percent Frequency for TTD.

#### **For online & street survey group: (200 respondents)**

From the responses above in Table 4-29, 39.0% (78 out of total 200) of respondents agree or strongly agree that they would think twice before giving out personal health information. There is a concern regarding the collection of medical data. This is in contrast to 49.0% (98) of respondents who disagree or strongly disagree cumulatively (feeling comfortable) that they would need to think twice before giving out personal health information to their service provider. They have less concern about the ways that EHR data were collected. It is important to note that 12.0% (24 out of 200) of the respondents are undecided on whether they have to think twice when service provider asks them for personal health information.

#### **Classroom survey group (189 respondents)**

From the responses above in Table 4-29, 41.3% (78 out of 189) of respondents agree or strongly agree that they will think twice before giving out private information. There is a concern (uncomfortable feeling) towards the collection of medical data. This is in contrast to 46.0% (87) of respondents who disagree or strongly disagree (feeling comfortable) that they have to think twice when service provider asks them for personal health information. About the same as the online and street survey, there is 12.7% (24) of the respondents are neutral or undecided on this question.

## Observations

The chart shows a bimodal result. There is a significant proportion of respondents who disagree or strongly disagree that they have to think twice when service providers ask me for personal health information. There is about the same portion of the online and street survey group as compared to the classroom survey group. Both groups are neutral to the questions that they have to think twice before providing personal health information.

### 4.6 Age Modeled via Career Stage

To have a meaningful discussion of the age of respondents, the author modeled the age variable by mapping it to career stage. Constructs and hypothesis are created so that meanings and interpretation of the survey results can be discussed.

From the table below, in the design of the survey (online, street and classroom), “Age” variable is divided into six group categories and is mapped onto three career stages. They are:

Group	AGE	Career stage
1	18-25	Early
2	26-35	
3	36-45	Mid
4	46-55	
5	56-65	Late
6	66+	

Table 4-30: Age group distribution and mapping to career stage.



Age Group	No. of respondents	%	Career Stage	No. of respondents	%
1	216	47.79	Early	332	73.5
2	116	25.66			
3	34	7.52	Mid	68	15.0
4	34	7.52			
5	40	8.85	Late	52	11.5
6	12	2.65			
<b>Total:</b>	<b>452</b>	<b>100</b>	<b>Total:</b>	<b>452</b>	<b>100</b>

Table 4-31: Results of age group distribution.

The division of the age variable into six groups is based on the patients' priority in their concern for privacy as affected by their social needs; career needs and lifestyles changes throughout their career life-cycle. It is hypothesized that social needs and lifestyle changes are associated with the career stages of a patient. Although the age group is divided into six groups from the raw data collection, we group a patient's career life cycle into three career stage clusters. They are early, mid and late career stages. The early career stage is composed of patients aged from 18 to 35 (age group 1 and 2). The mid-career stage cluster is patients from 36 to 55 years of age (age group 3 and 4). The late-career stage cluster is patients aged 56 and above (age group 5 and 6)

Because of the intention to capture these dimensions, the age distribution among these three career clusters is slightly different. For example, the early-career group as 17 years in age span, the mid-career stage cluster has a 20 years age span and the late-career stage cluster has the most 15 years age span and perhaps, more as many respondents may work until they are 70 years of age.

The reasons for such age allocation are based on the following constructs. It is also based on the patients' perceived cost and benefits in exposing their private information within their career stage cluster. These perceptions of exposure can be either through employment or their social needs if they are not employed.

It is noted that the following constructs and hypothesis are used to create a framework for studying the response of the patient (survey respondents) rather than as a firm statement to be proved. The cost of damages due to information privacy exposure and the benefits of employment or social needs will form the analytical framework for studying the patient's concerns about information privacy.

#### **4.6.1 Early Career Cluster: (18 – 35 years. old)**

##### Group 1 (18 – 25 years old)

**Construct 1:** The concern of privacy in age group one is dominated by social acceptance.

This age group may have the following dimensions that influence their decision on privacy. They are:

- (1) Many patients in this age group may still be a student, part-time worker and may not yet be working in a full-time career. Therefore, their concern about privacy may be reflected in their social needs.
- (2) It is very common for this age group to share information via social media, texting, and sharing of pictures. Therefore they conform to social norms regarding the privacy of their information.
- (3) Communication in this age group is commonly seeking friendship and endorsement (social recognition) from others, therefore lowering their privacy requirements.
- (4) Members of this age group are very comfortable, and at ease with using information technology, therefore they do not have as many concerns regarding their information being proliferated in the social group.
- (5) The attitude of there is “nothing to lose” in sharing or exposing their private information as they often neither have the experience nor able to foresee the impact of losing their private information.

- (6) Many members in this age group are still seeking or establishing their social identity (such as group acceptance, their own perception of themselves), therefore will trade privacy for group acceptance.

**Assertion 1:** Patients in this age group 1 (18-25 years old) have fewer concerns about their private information than other age groups.

Assessment: CFIP dimensions for testing of the hypothesis are “Collections” and “Unauthorized Access.” Other contributive factors to be reviewed based on the result of data analysis.

Group 2 (26 – 35 years old)

**Construct 2:** The privacy concerns for age group two are dominated by the early stage of employment prospects.

There is increasing privacy concern in the second group (group two) of the early career stage group when compared to those at earlier stages of their careers. The mid-career group is concerned with building up their career whereas the early-career stage group (age group 1) is more concerned with their social acceptance and monetary benefit.

The following factors may affect the decision of patients in the age group two.

- (1) Patients from group 2 will generally not be eligible to be covered as dependents in the public insurance scheme in Ontario.
- (2) Youth employment subsidy may also be reduced as they started to accumulate work experience and would be eliminated by age 28.
- (3) There is a priority to establish a stable income. This is achieved by searching and settling for a job or a career that has good prospects.
- (4) The seeking of peer-to-peer friendship and endorsement (social recognition) from others in the age group one may now be redefined as co-worker's social acceptance and recognition of their employment.
- (5) The cost of privacy exposure may affect their chances of getting a job or the opportunity for advancement within a business organization.

**Assertion 2:** There is increased concern about information privacy in the age group two when compared to age group one within the early-career stage.

#### **4.6.2 Mid-Career Stage Cluster: (36 – 55 yr. old)**

The mid-career stage is composed of age groups 3 (36 – 45), and group 5 (46 – 55) with a career stage spanning of 20 years.

**Construct 3:** The concern of privacy in career stage is dominated in the pursuit of employment benefits and wealth building.

Patients in the mid-career stage cluster may already have years of work experience. They are at a stage of meeting life's demands on their income and are becoming more focused on wealth accumulation. For patients that are not working, they could have by now a 15+ year of social experience in their adulthood. In either case, both groups will try to consciously increase their benefits and reduce any cost of privacy exposure that could affect their growth opportunity in career or their social recognition.

**Assertion 3:** Patients in the mid-career stage will have concerns for information privacy in EHR on an error, collection and improper access in the CFIP dimensions with less concern on the Secondary Use of data.

#### **4.6.3 Late-Career Stage Cluster: (ages 56+)**

Late-career group composed of age groups six (56 – 65) and group 7 (65+) with a career stage cluster spanning of mostly up to 15 years. Patients in this group are dominated by the concerns of the exposure to their health issues that could jeopardize their employment and in the final stages building of better employee benefits and preparation for retirement.

**Construct 4:** Patients in this late-career stage are dominated by the concerns of privacy exposure of their health information that affects the current career and the benefits of retirement.

**Assertion 4:** Patients in this late career stage are more concerned with “Error” and “Unauthorized Access” of their EHR information.

## 4.7 Results of Findings in Career Stage Cluster

### 4.7.1 Concerns of Error

The concern about Error by career stage			
	Early	Mid	Late
Disagree	1	1	0
Agree	322	67	52
Undecided	9	0	0
Total no.	332	68	52
% of Patients' concern of error /career stage			
	Early	Mid	Late
Disagree	0.3	1.5	0.0
Agree	97.0	98.5	100.0
Undecided	2.7	0.0	0.0
Total	100.0	100.0	100.0

Table 4-32: Results of the age group in CFIP error dimension.

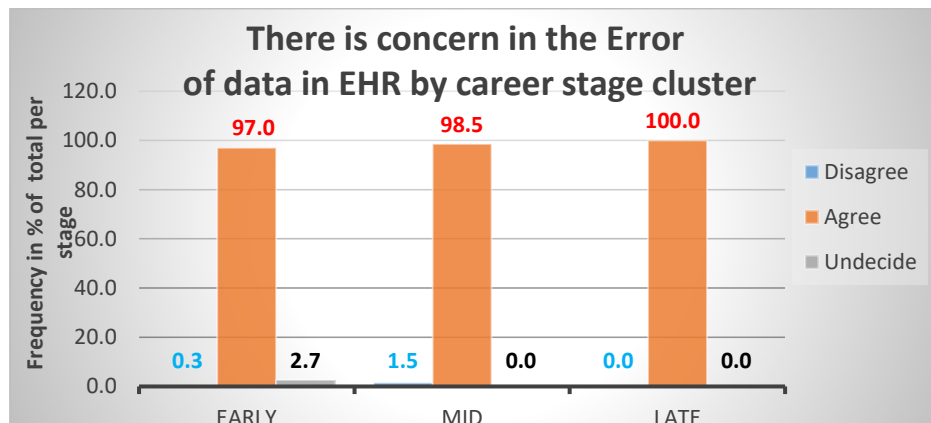


Figure 4-18: Concerns of Error by career stage cluster

## Observations

Across all the three career stages (Early: age 18-35; Mid: 36-55 and Late: 56+), there is a high percentage, 97% or above agreed that there is a concern with Error in EHR

### **Early-career stage cluster (age 18-35):**

There are 97% (322 out of 332) respondents surveyed in this group agreed that there is concern about Error of data in EHR. Only 0.3% (1 out of 332) respondents surveyed were not concerned with Error of data in EHR, and 2.7% (9 out of 332) respondents were undecided.

### **Mid-career stage cluster (age 36-55):**

The survey showed that 98.5% (67 out of 68) respondents agreed that there is a concern with Error of data in EHR. There is only a 0.3% (1 out of 68) of respondents surveyed was not concern with data Error in EHR. No respondent was undecided.

### **Late-career stage cluster (age 56 and above):**

All (52 out of 52) respondents surveyed agreed that there is a concern with Error of data in EHR.

#### 4.7.2 Concerns of Improper Access

The concern about improper access by career stage			
	Early	Mid	Late
Disagree	2	0	1
Agree	322	67	49
Undecided	8	1	2
Total no.	332	68	52
% of Respondents' concerns of improper access by age group			
	Early	Mid	Late
Disagree	0.6	0.0	1.9
Agree	97.0	98.5	94.2
Undecided	2.4	1.5	3.8
Total	100.0	100.0	100.0

Table 4-33: Results of the age group in CFIP improper access dimension.

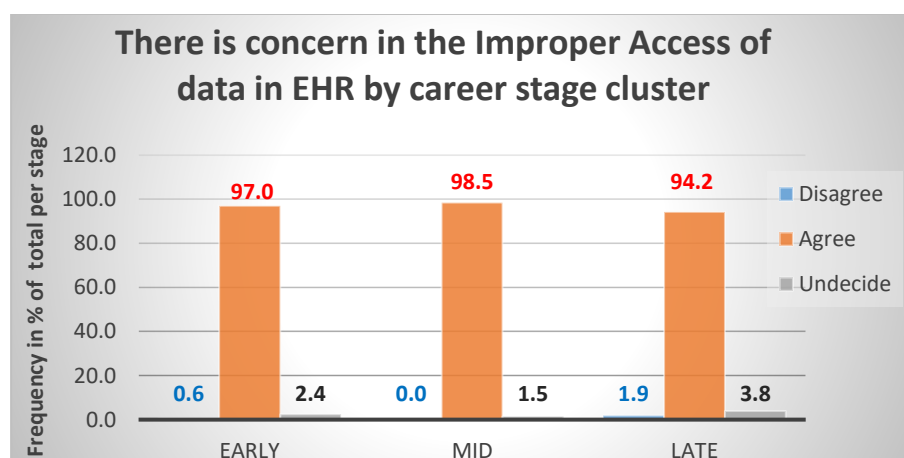


Figure 4-19: Concerns about improper access to data by career stage cluster

##### Early-career stage cluster (age 18-35):

Among the early-career respondents surveyed, 97% (322 out of 332) agreed that there is a concern with improper access to data in EHR. 0.6% (2 out of 332) respondents surveyed who were not concerned with improper access to data in EHR and 2.4% (8 out of 332) respondents were undecided.

**Mid-career stage cluster (age 36-55):**

Among the mid-career respondents surveyed, 98.5% (67 out of 68) agreed that there is a concern with improper access to data in EHR. No respondent disagreed, and one was undecided.

**Late-career stage cluster (age 56 and above):**

Among the late-career respondents surveyed, 94.5% (49 out of 52) agreed that there is a concern with improper access to data in EHR. There were 1.9% (1 out of 52) respondents surveyed did not have a concern with improper access to data in EHR, and 3.8% (2 out of 52) respondents were undecided.

**4.7.3 Concerns about Secondary Use**

<b>The Concerns about Secondary use by career stage</b>			
	<b>Early</b>	<b>Mid</b>	<b>Late</b>
<b>Disagree</b>	1	1	0
<b>Agree</b>	325	66	50
<b>Undecided</b>	6	1	2
<b>Total no.</b>	332	68	52
<b>% of Patients' concerns of Secondary Use by career stage</b>			
	<b>Early</b>	<b>Mid</b>	<b>Late</b>
<b>Disagree</b>	0.3	1.5	0.0
<b>Agree</b>	97.9	97.1	96.2
<b>Undecided</b>	1.8	1.5	3.8
<b>Total</b>	<b>100.0</b>	<b>100.0</b>	<b>100.0</b>

Table 4-34: Results of the age group in CFIP secondary use dimension.



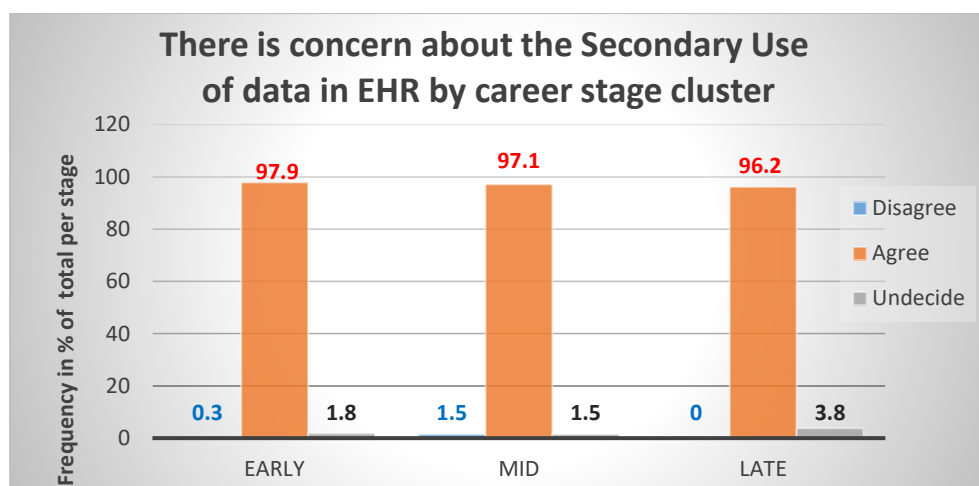


Figure 4-20: Concerns about the secondary use of data by career stage cluster.

### **Early-career stage cluster (age 18-35):**

Among the 332 respondents surveyed in the early-career stage cluster, 97.9% (325 out of 332) agreed that there is a concern with Secondary Use of data in EHR. Just 1 out of 332 respondents surveyed was not concerned with the secondary use of data in EHR and a small number of respondents 1.8% (6 out of 332) were undecided.

### **Mid-career stage cluster (age 36-55):**

Among the 68 respondents surveyed in the mid-career stage cluster, 97.1% (66 out of 68) agreed that there is a concern with the secondary use of data in EHR. Only 1 out of 68 (1.5%) of respondents surveyed was not concerned with the secondary use of data in EHR, and equally, 1 out of 68 respondents was undecided.

### **Late-career stage cluster (age 56 and above):**

Among the 52 respondents surveyed in the late-career stage cluster, 96.2% (50 out of 52) agreed that there is a concern with the secondary use of data in EHR. None of the respondents disagreed that there is no concern with the secondary use of data in EHR and 3.8% (2 out of 52) respondents were undecided.

#### 4.7.4 Concerns of Collection

Concerns of Collection by career stage			
	Early	Mid	Late
Disagree	83	21	20
Agree	115	28	20
Undecided	134	19	12
Total	332	68	52
% of Patients' concerns of collection per career stage			
	Early	Mid	Late
Disagree	25.0	30.9	38.5
Agree	34.6	41.2	38.5
Undecided	40.4	27.9	23.1
Total	100.0	100.0	100.0

Table 4-35: Results of the age group in CFIP collection dimension.

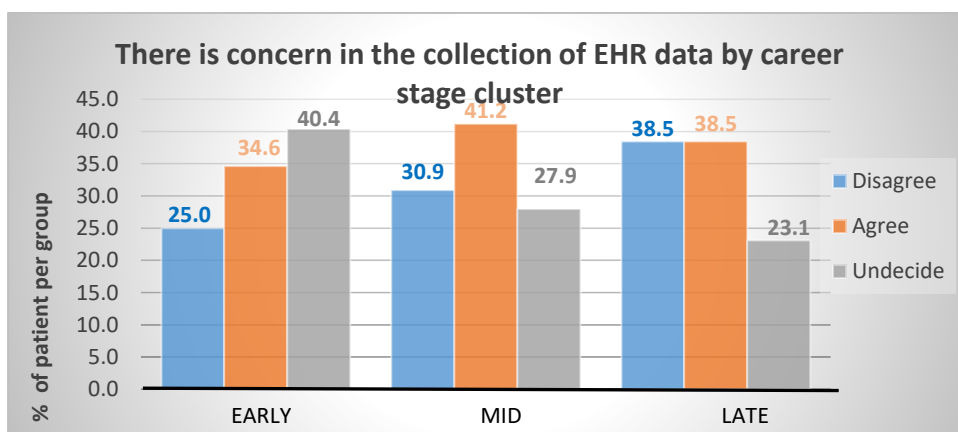


Figure 4-21: Concerns of a collection of data by career stage cluster

#### Early-career stage cluster (age 18-35):

Among the 332 respondents surveyed in the early-career stage cluster, 34.6% (115 out of 332) agreed that there is a concern with over-collection of data in EHR. 25.0% (83 out of 332) respondents surveyed did not concern with over-

collection of data in EHR, and 40.4% respondents (134 out of 332) were undecided.

**Mid-career stage cluster (age 36-55):**

Among the 68 participants surveyed in the mid-career stage cluster, 41.2% (28 out of 68) agreed that there is a concern with over-collection of data in EHR. 31.8% of respondents disagreed, and 28.0% of respondents were undecided.

**Late-career stage cluster (age 56 and above):**

Among the 52 respondents surveyed in the late-career stage cluster, 38.5% (20 out of 52) agreed that there is a concern with over-collection of data in EHR. An equal number of 38.5% (20 out of 52) respondents surveyed were not concerned with over-collection of data in EHR, and 23.1% (12 out of 52) respondents were undecided.

**Summary of findings in age as modeled through career stage**

From the survey results presented from Figure 4 -18 to Figure 4-20, there is no career stage (age) difference across the privacy concerns of “Error”; “Improper Access” and “Secondary Use” in the CFIP dimensions. In these three dimensions, respondents across all career stage (age) has a high percentage (a minimum of 95%) agree that there is a privacy concern. However, in the “Too much collection” dimension, each of the three career stages exhibited a similar pattern of the percentage of disagree, agree and undecided in the response categories as presented in Figure 4 -21.

## **4.8 Response by Gender**

There were no pre-assumptions of a reference gender of either male or female when setting up the survey or for later interpretation. We expect the result of data to expose any potential significance of the gender with relationship to the

four CFIP categories. Table 4-36 below shows the result of the four CFIP dimension by gender.

The error of EHR data				
	Not concern	Concern	Neutral	Total:
Male	1	268	1	270
Female	1	174	0	175
No. of Patient	2	442	0	444
% Male	0%	99%	0%	100%
% Female	1%	99%	0%	100%
Improper Access of EHR data				
	Not concern	Concern	Neutral	Total:
Male	2	267	9	278
Female	1	172	2	175
No. of Patient	3	439	11	453
% Male	1%	96%	3%	100%
% Female	1%	98%	1%	100%
Secondary Use of EHR data				
	Not concern	Concern	Neutral	Total:
Male	1	270	7	278
Female	1	172	2	175
No. of Patient	2	442	9	453
% Male	0%	97%	3%	100%
% Female	1%	98%	1%	100%
Too much Collection of private information				
	Not concern	Concern	Neutral	Total:
Male	67	100	111	278
Female	57	63	55	175
No. of Patient	124	163	166	453
% Male	24%	36%	40%	100%
% Female	33%	36%	31%	100%

Table 4-36: Result of the four CFIP dimension by gender.

In Table 4-36 above, it shows that the percentage of female and male respondents are about same on three of the four privacy concern in the CFIP dimensions over the EHR privacy.

However, female respondents have scored a higher percentage on the “Not Concerned” of privacy in the CFIP dimension of “too much collection” of private information than that of the male respondents. The author noted that in this dimension of “too much collection,” the result is quite different from the other three CFIP dimensions. In this dimension, more female (33% female vs. 24% male) respondents have expressed their attitude that they are less concern with too much data collection.

Examining the Likert scale of “neutral,” in Table 4-36, the percentage of female students that took on the “neutral” position is less among all categories. This suggests that female participants have a stronger opinion than the male participants. It is important to point out that in contrast to all the other CFIP three dimensions, the “too much collection” dimension suggests the respondents are divided (about in one-third) among each of the three categories of “no concern”, “concern” and “neutral” categories.

In the category of “no concern,” there is no significant difference between female and male in the “secondary use,” “improper access” and the “error of information” of EHR. The number of respondents is small (2 or less) in these three categories. However, in the CFIP dimension of “too much collection of private information,” the percentage of female respondents are nine percent higher than that of the male respondents in the category of “Not Concern.” Virtually all of both genders rated high-level (95% - 99%) of “concern” in each of the four dimensions except the “too much collection” dimension that received a 36% for both genders. This is incongruent to most of the survey results that female respondents have a high level of privacy concern. Further discussion will be found in Chapter Seven for the “too much collection” dimension related to the female respondents.

## **4.9 The result of Scenario Questions**

Scenario questions were used to collect data as to the degree of patients' privacy concern regarding their willingness to take countermeasure or actions to reduce the impacts of their exposure. As the primary contacts of EHR to the patients are their service provider, the questions are focused on answers that patients can relate. The answer to each question is set in the successive severity of response. A severe response requires more effort and willingness for the patient to countermeasure the exposure.

### **4.9.1 Purpose of Scenario Questions**

One of the primary objectives of this research is to understand the respondents' attitude towards their concerns about the information privacy of their EHR record. An effective way to understand attitudes is to survey the respondents' belief in their actions given a scenario. (The survey is designed to obtain a response that is based on the severity of actions taken). An answer of 1 means that the respondent chooses a least severe action and an answer of seven is the most severe action from a list of choices of action. This answer measures the willingness of the patient to spend time and resources to respond to the severity of the action towards a given breach of privacy. The followings are the six scenarios studied in this research.

### **4.9.2 Share Information Without Consent (SSWC)**

Scenario 1: If your doctor shares your health information with a third party (such as an insurance company or an employer that provides you with benefits or a salary) WITHOUT your consent, you would most likely:

- 1- Do nothing
- 2- Express your concern to your doctor
- 3- Ask your doctor to take corrective action to your satisfaction
- 4- Call the third party to tell them they have no rights to use your information

5- File a complaint with the Privacy Commissioner and request their assistance

6- Seek legal advice

7- Sue your doctor for damages caused

### Result:

SSWC	% of total respondents							Mean score	Standard Deviation	Total number of respondents
Answer:	1	2	3	4	5	6	7	4.0		
Online + Street	3.6	19.2	25.4	5.2	19.2	19.7	7.8	4.1	1.89	193
Class-room	6.4	17.0	22.5	4.6	17.0	19.7	12.8	4.2	1.84	218

Table 4-37: Frequency table for scenario SSWC.

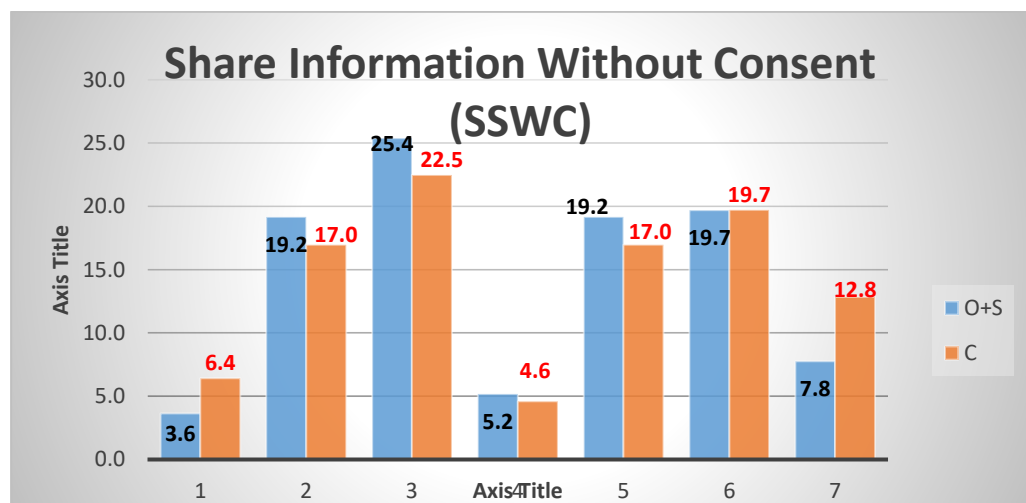


Figure 4-22: Frequency in percentage for SSWC

From the data above, it is clear that only a small percentage of respondents will “do nothing” given the scenario. The classroom respondents (classroom) will do nothing (6.4%) more frequently as compared to the online and street survey respondents (3.6%). However, on the other end of the action spectrum, 12.8%

of the classroom respondents will sue the service provider (doctor) for damage as compared with 7.8% of the online and street survey respondents.

#### 4.9.3 Disclosure May Result In Social Rejection (SDSR)

Scenario 2: Suppose you have contracted a disease that is normally transmitted sexually. You consider your medical condition private, and your family doctor does not know about it. Disclosing your condition will invite a treatment program that might result in you being rejected by your partner and friends. During your regular check-up with your family doctor, you would most likely:

- 1- Give the doctor full details of this private medical condition, so that he can refer you to a specialist
- 2- Ask him whether it is important for him to know
- 3- Bring up the condition to gather information but do not say that it applies to you, such as saying, a friend has this problem
- 4- Tell him part, but not all, of the private information and
- 5- Not let your doctor know at all

#### Result:

SDSR	% of total respondents					Mean Score	Standard Deviation	Total number of respondents
Answer:	1	2	3	4	5	3.0		
Online + Street	73.1	9.8	7.3	8.3	1.6	1.6	1.18	193
Classroom	75.4	9.0	6.6	7.6	1.4	1.5	1.09	211

Table 4-38: Frequency table for scenario SDSR.



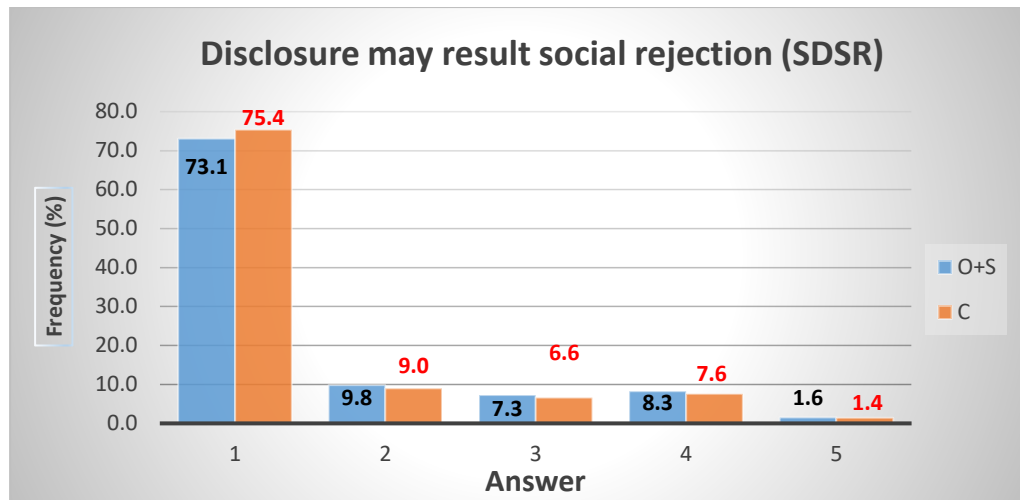


Figure 4-23: Frequency in percentage for SDSR .

It is evident in this scenario that closes to 75% of the respondents from both the online and street survey, as well as classroom groups, consider getting help in healing from the disease is far more important than social embarrassment and rejection. About 9% of both groups of respondents will still take some precaution in guarding their privacy by asking if it is important for the doctor to know.

Both answers 3 and 4 in this scenario question refers to telling the service providers part of the private information about the illness. In these two answers, there are 15.2% (7.3% + 8.3%) of the online and street survey respondents will try to find out more on the treatment without disclosing their privacy compares to a lower percentage of 14.2% (6.6% + 7.6%) of classroom respondents. It is noted that as part of the rationale for the disclosure of private information the respondents perceive that the disclosure is a requirement of treatment.

#### 4.9.4 Disclose may result in a financial loss (SDFL)

Scenario 3: Suppose you are a professional driver shipping goods between Canadian provinces. A nurse makes you aware of the very high possibility that you are suffering from Obstructive Sleep Apnea (OSA) and you believe the nurse's observation is true. Such disease could cause you to fall asleep while operating a motor vehicle such as your commercial trailer. Your doctor told you

that he is required to report OSA to the ministry of transportation if his patients suffer from it. You know that you could lose your driving privileges and your job as a result. What will you let your doctor know?

- 1- You will give him the full details of your OSA and hope that the disease is treatable
- 2- You will tell him that you might have a mild case of OSA
- 3- You will tell him that you are not sure if you have OSA but you want to find out more information
- 4- You will take precautions against such disease, but do not tell the doctor about your OSA
- 5- You will never tell anyone about the disease regardless of the situation.

**Result:**

<b>SDFL</b>	<b>% of total respondents</b>					<b>Mean Score</b>	<b>Standard Deviation</b>	<b>Total number of respondents</b>
<b>Answer:</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>3.0</b>		
<b>Online + Street</b>	45.5	4.7	38.7	9.9	1.0	<b>2.2</b>	<b>1.32</b>	<b>191</b>
<b>Classroom</b>	51.9	4.2	34.3	8.8	0.9	<b>1.5</b>	<b>1.16</b>	<b>216</b>

Table 4-39: Contingency table for scenario SDFL.

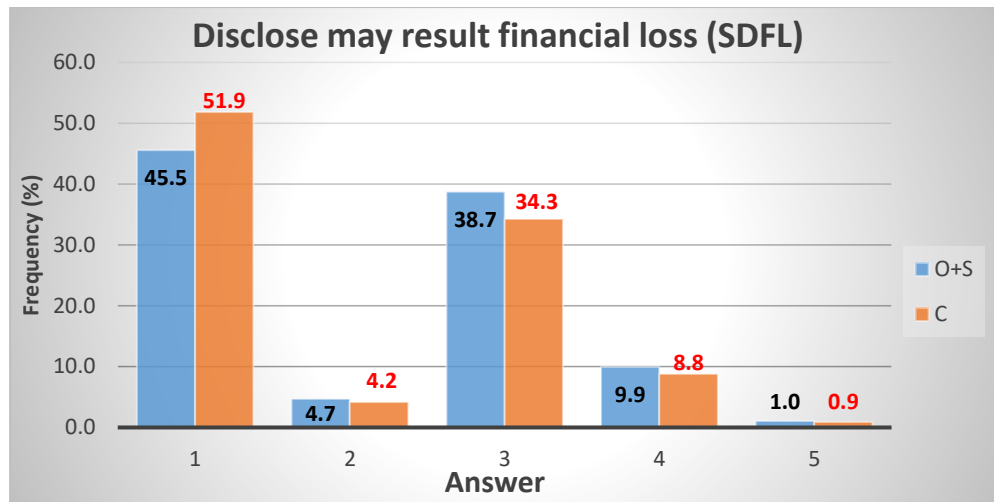


Figure 4-24: Frequency in percentage for SDFL.

There is close to half of the respondents from both groups, choose to give full details of their disease in the hope of treating the disease and willing the risk of the potential loss of income. A little over one-third of the respondents from both groups want to get more information and still protect their privacy by claiming that they are not sure if they have the OSA disease. Some 10.0% of the respondents guard their privacy and take measure for precautions.

#### 4.9.5 Disclosure with countermeasure (SDWC)

Scenario 5: Suppose you have a medical condition that you want to keep private because disclosure will embarrass you. The doctor assures you that the Electronic Health Record about his patient's private condition will be kept private, but you see that the receptionist in your doctor's office reads patient health records to satisfy his/her curiosity and pass the time. The receptionist is also a resident of your community and is an active member. Will you tell the doctor about your medical condition that you consider private?

- 1- Yes, but ONLY if that medical receptionist is not on-duty that day
- 2- Yes, but will also make a complaint to the doctor about the wrongdoing of that receptionist
- 3- Yes, but in order to avoid the receptionist, you will go through the trouble of seeing the doctor in another of his clinics even if it is an hour away
- 4- No, you do not trust the doctor anymore, as s/he does not have control over his policy of keeping the EHR private
- 5- No, you will change to another doctor, as there are other doctors available

## Result:

SDWC	% of total respondents					Mean Score	Standard Deviation	Total number of respondents
Answer:	1	2	3	4	5	3.0		
Online + Street	7.7	61.2	8.2	9.7	13.3	2.6	1.23	196
Classroom	16.6	55.3	7.4	8.8	12.0	2.4	1.27	217

Table 4-40: Contingency table for scenario SDWC.

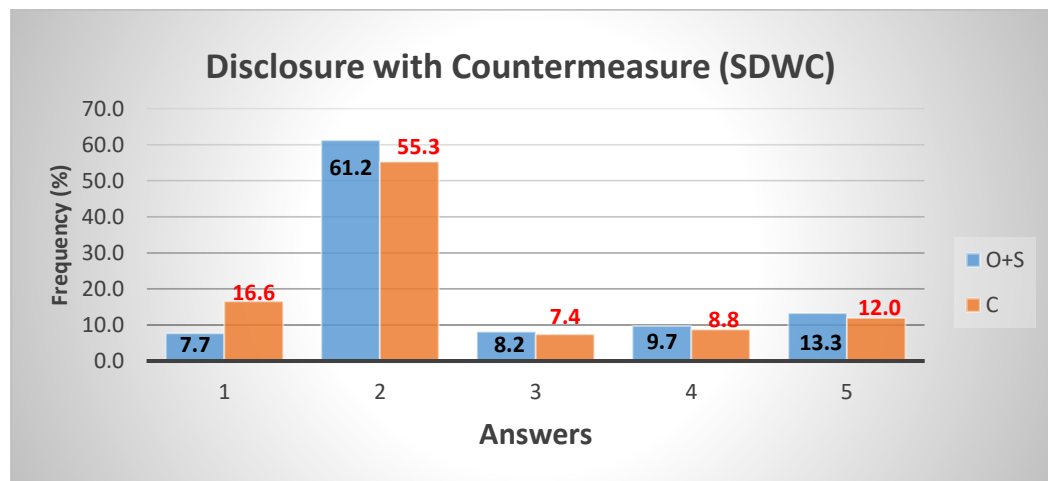


Figure 4-25: Frequency in percentage for SDWC

About 55% of both groups will inform the doctor of their potentially embarrassing disease and complain about the apparent breach of privacy practiced by their staff for which it breaks the assurance of privacy by the doctor. This suggests that respondents have trust with the doctor and believe that the doctor has the capability and willingness to correct the breach of privacy in the medical office. About 9.5% of respondents do not trust the doctor, and about 12% will take action by changing doctors. Changing doctors in Greater Toronto Area is not an easy as there is a shortage of the doctor and many doctors do not take new patients.

#### 4.9.6 Disclosure when in an emergency (SDWE)

Scenario 4: Suppose you have a medical condition (disease) that you consider private and that is known only to you. One day, you are being treated in an emergency room for an apparent heart attack. When will you let the emergency doctor who provides services to you know about this medical condition (disease)?

- 1- Let him know right away regardless of your medical condition
- 2- Let him know if you think that by giving him your private medical condition, you will help him to provide better care for you.
- 3- Let him know if you think you are in a life-threatening condition regardless of whether this will be of any use to him
- 4- Don't tell him anything until you find out the severity of your current condition
- 5- Never, even if you are in a life-threatening condition

#### Result:

SDWE	% of total respondents					Mean Score	Standard Deviation	Total number of respondents
Answer:	1	2	3	4	5	3.0		
Online + Street	50.5	36.1	7.2	6.2	0.0	1.6	1.69	194
Classroom	57.4	28.7	11.2	2.8	0.0	1.7	0.80	240

Table 4-41: Contingency table for scenario SDWE.

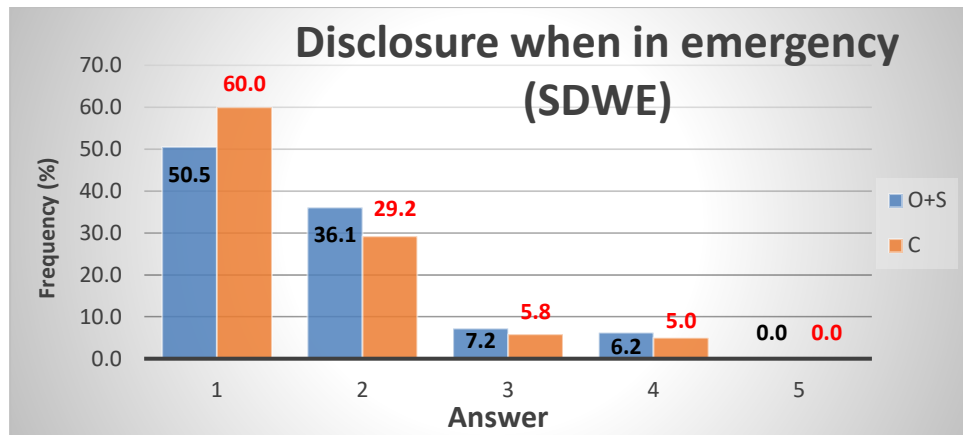


Figure 4-26: Frequency in percentage for SDWE

Out of 434 respondents surveyed, none would risk their life to guard their privacy. Adding up answers 1 and 2 above, there are about 86.6% in O+S group, and 89.2% in C group of respondents would let the doctors know even if they think it was not a life-threatening situation. This suggests a trust to the service providers. There is, however, about 13.4% in O+S group and 10.8% in C group that would first assess the severity of the illness before letting the service provider knows about their illness that they have been kept private.

#### 4.9.7 Control data privacy (SCDP)

Scenario 6: Suppose you regularly manage information using the Internet, (e.g., pay bills electronically, check banking accounts). If you were allowed to manage the accuracy of your Electronic Health Record, what would you likely do?

- 1- Do nothing. You are not interested in having any access to your Electronic Health Record
- 2- You would log in and check that your information is accurate, especially after major medical tests and procedures.
- 3- You would check the accuracy of information and request changes to incorrect information by the service provider
- 4- You would like to have the ability to indicate which information you would like to keep private
- 5- You would like to have a “Privacy Profile” in the system where you can specify what kind of information should be kept private

## Result:

SCDP	% of total respondents					Mean Score	Standard Deviation	Total no. of respondents
Answer:	1	2	3	4	5	3.0		
Online + Street	4.6	26.2	28.7	6.2	34.4	3.4	1.41	195
Classroom	6.1	25.8	28.3	6.1	33.8	3.4	1.31	198

Table 4-42: Contingency table for scenario SCDP.

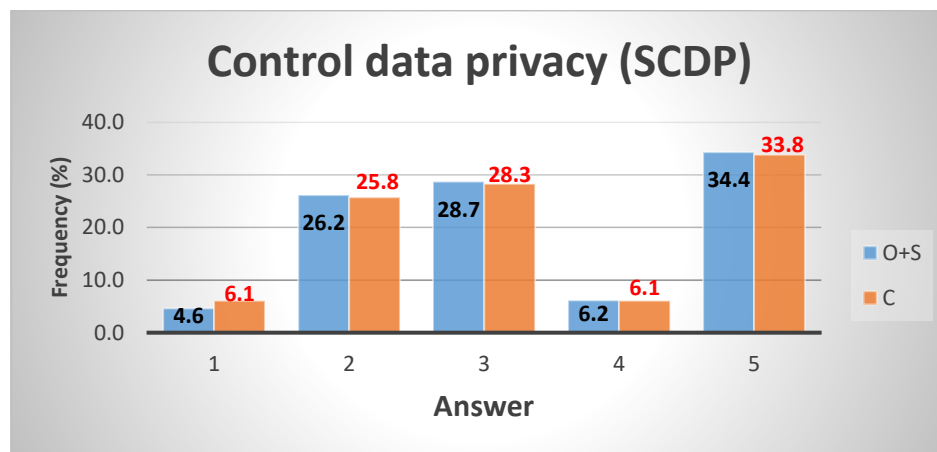


Figure 4-27: Frequency in percentage for SCDP.

Given the scenario that patients can access EHR, about 26% of respondents (patients) are willing to take the time to check the accuracy of their EHR to ensure that data is accurate. Another 27% will take steps to inform the service provider to correct the accuracy of data. Significantly, at least 33.8% of the respondents welcome the ability to control the privacy of their data in EHR with a privacy profile that they can specify. This question revealed a strong intention from auditing of data to deciding who can see the data by specifying a privacy profile.

#### 4.10 Overall Attitude Towards Service Provider

Based on the literature review and epistemological behavioral theory, observation and experience influence beliefs. A firm belief influences attitudes and attitudes influence action. Collective or repetitive action forms behavior. By asking a question of a participant's belief whether a doctor can keep their data secure and private, we can gain some understanding of the answers provided by the respondents. A more comprehensive assessment and analysis will be performed in Chapter Seven, the discussion chapter.

##### 4.10.1 Provider Can Keep Data Secure And Private (DSP)

Variable	Survey Question
DSP	I think that service providers can keep my data secure and private

DSP is a modulating variable measuring the attitude of respondents' belief toward their provider. Such an attitude influences the result of the dependent variable of "willingness to provide private information." This question asks two points, secure and private. The results of the pilot surveys showed that some respondents have no idea if the provider will be able to keep their data private but believed that doctor could keep their data secure. Although security and privacy are two different constructs in this thesis, it is generally agreed that a higher level of security will often produce a state of higher privacy.



## Result:

DSP	% of total respondents per Likert Scale					Mean Score	Standard Deviation	Total no. of respondents
Likert Scale:	1	2	3	4	5	3.0		
Online + Street	2.0	15.6	26.6	37.2	18.6	3.5	1.08	193
Classroom	6.0	13.5	31.0	34.5	15.1	3.4	1.08	218

Table 4-43: Result of the 5-point Likert scale on DSP – Provider can keep data secure.

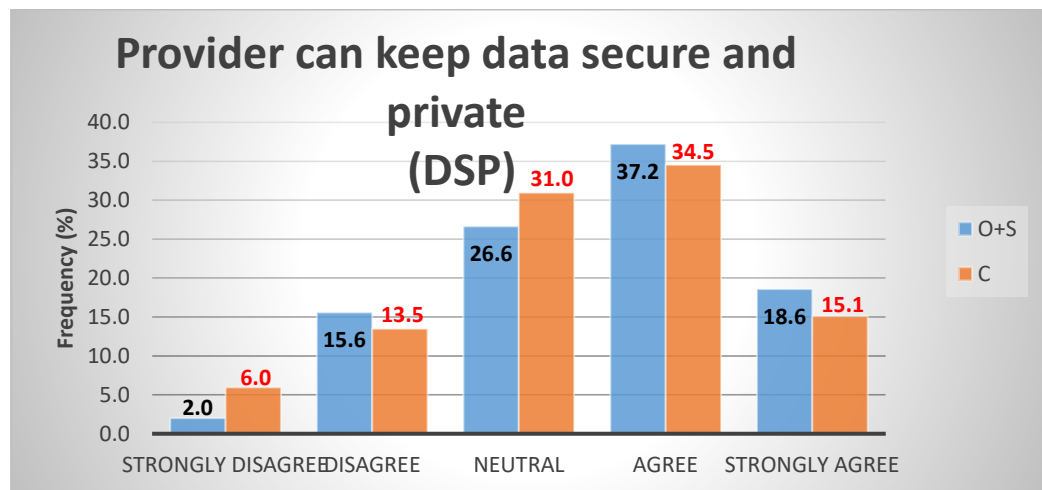


Figure 4-28: Frequency in percentage for DSP

Overall, 55.8% of the online and street survey respondents have a positive belief that provider can keep their data in EHR private. This is in contrast to the classroom survey that shows a 49.6% positive belief towards the doctor ability to keep their EHR data private.

There is a 26% and 31% of respondents from the O+S and C groups respectively do not have any opinion on this question.

Quite a large group (17.6% and 19.5% from O+S and C groups respectively) strongly disagree or disagree that providers can keep their data in EHR secure and private.

#### 4.10.2 Willing to Give Information if Sickness Worsens (WIW)

This question is designed to explore if there is a shift of willingness to give up privacy (measured from the answer pattern on the 5-point Likert scale) when a modulating variable of “sickness worsens” is applied.

Variable	Survey Question
WIW	I am willing to give more health and other private information to the providers if my illness becomes severe.

#### Result:

WIW	% of total respondents per Likert Scale					Mean Score	Standard Deviation	Total no. of respondents
Likert Scale:	1	2	3	4	5	3.0		
Online + Street	0.5	3.6	9.6	40.6	45.7	4.3	0.93	197
Classroom	3.2	5.6	15.9	40.1	35.3	4.0	1.01	252

Table 4-44: Result of the 5-point Likert scale on WIW- Willingness to give information

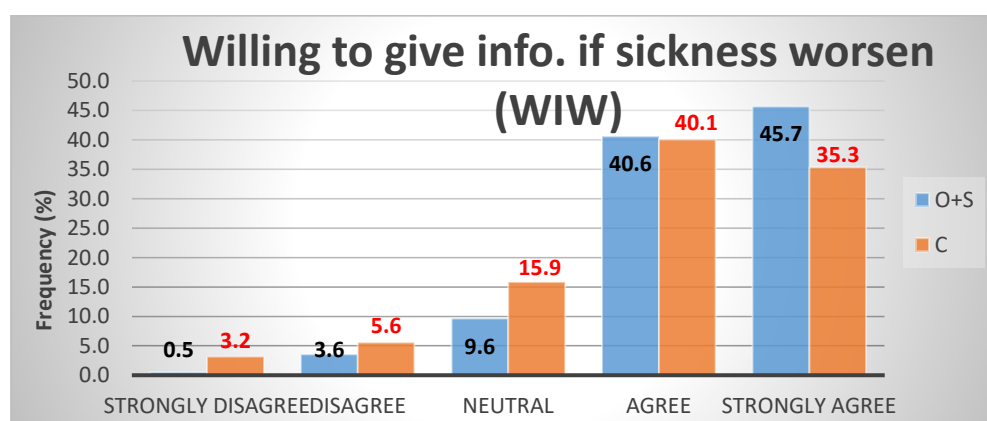


Figure 4-29: Frequency in percentage for WIW

It is clearly shown from the result that 86.3% and 75.4% of respondents from O+S and C groups respectively shown a belief of agree and strongly agree that they will trade off their privacy when their sickness worsens. When comparing this to the previous modulating variable of DSP (Data can be kept secure and

private), a distinct pattern of shifting towards the positive side of the Likert scale is found in WIW variable.

#### **4.11 Emerging Themes**

The following emerging themes were observed from the patient survey. Further analysis and integration of theme and variable into the four CFIP dimensions can be found in Chapter Seven.

As shown in Figure 4-30 below, in the area of concern in the errors of EHR data, the result is very significant in that most respondents to have a concern regarding the secondary use of their EHR data. This implies that there is a concern about the unauthorized use of EHR other than matters related to helping patients in the healthcare. It also indicated from the data that the concern is across the whole spectrum of the age groups across both genders.

From the survey result, it also appears that respondents generally trusted their service provider. When sickness worsens, respondents have opted for trading their privacy for a perceived better treatment of their illness. They are willing to volunteer more of their private information to their service provider, mainly if they believe this will allow the service provider to deliver better care.

The survey results also suggest that most patients (59.8% in O+S and 49.6% in C) agree that provider can keep their data secure and private (DSP). However, it also shows that 17.6% of Online and street and a 19.5% in Classroom that do not agree that their provider can keep their data secure and private.

Of the four CFIP dimensions namely, Collection, Error, Improper Access and Secondary Use of data. The Improper Access category has a significantly higher proportion of no-concern (48.3%) as compared to concern (30.7%). There is, however, 21.0% of the responses are in the undecided category that makes it significant in considering the result.

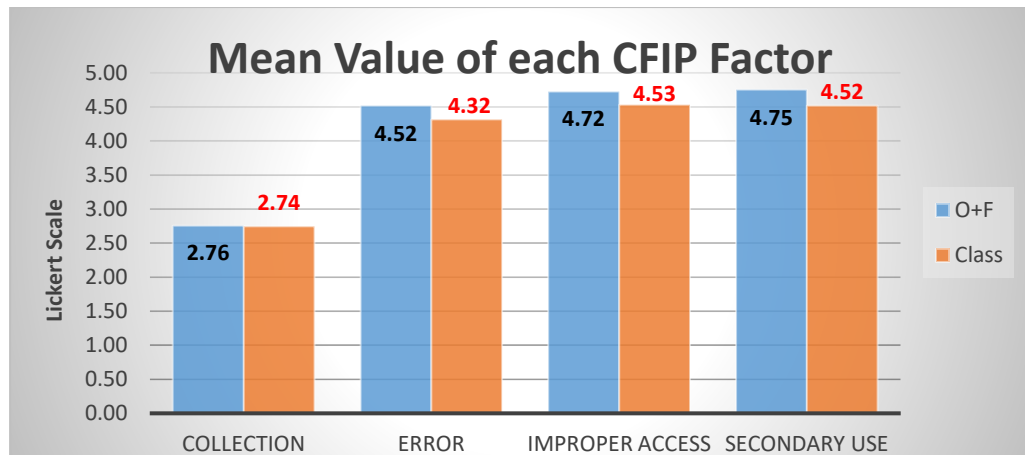


Figure 4-30: Overall survey result of the CFIP dimensions.

It is clear that respondents are very concerned with the secondary use of data (93.4%), and unauthorized access (95%) errors in data (91%) and would like to see the restriction of access to their data as evidenced in the scenario variable SCDP (Control Data Privacy).

These basic statistics form a framework to correlate the second part of the survey where respondents expressed their behavioral decision in their concerns about their privacy to EHR data.

#### 4.12 Preliminary Findings on patient's response towards the research sub-questions

The author examines the research sub-questions first as the scope is smaller and the questions are more focus than the primary research question. The primary research question comprises a more substantial body of knowledge. The main research question will be addressed in Chapter Seven after analysis of all sub-questions and findings. This section reveals the response only from the patient's side. Therefore, any potential triangulation types of findings (as per research design in Section 3.9) such as type 2 (T2P) or type 3 (T3P) findings

will be examined in Chapter Seven when the Triangulation design is used to converge all preliminary findings (PF).

Findings in this chapter will be considered preliminary until an analysis is done in Chapter Seven. Some preliminary findings may be combined or recategorized to form a Type 1; 2 or 3 finding. By using the Triangulation design as discussed in Section 3.9, the findings will first be labeled as Preliminary Findings (PF) following with Finding number as shown below for each of the empirical research from Chapter 4 Patients; Chapter 5 Providers and Chapter 6 Providers. In Chapter 7 after critical examination and convergence of the preliminary finding, the Triangulation result of Type 1, 2, and three findings will be formulated.

**[PF1]:** (Preliminary Finding 1): There are privacy concerns on all four CFIP dimensions.

**[PF2]:** Most patients will give out private information if sickness worsens

**[PF3]:** 55.8% of the online and street survey respondents trusted that provider could keep their data in EHR private.

**[PF4]:** There is no difference in gender among three of the four CFIP

**[PF5]:** There is no difference in the career stages (age groups) on three of the four CFIP dimensions except the “too much collection” dimension.

**[PF6]:** 34% of patients would like to have some control of their EHR data by specifying a privacy profile.

#### **4.13 Other Observed Preliminary Findings**

In addition to the attitude survey on the privacy concerns on EHR, part two of the survey asks the respondent to indicate their actions and behavior with a given a list of scenarios. The choice of answers in each question is a list of increasing severity of respondents’ action towards ramification of the problem.

As discussed in Section 4.12, the followings are additional preliminary findings of the patient in their choices of behaviors when their privacy is deemed violated by service providers:

**[PF7]:** Most patients (93%) will take action towards providers if privacy is violated.

Most respondents (93%) will take action towards providers if privacy is violated. Moreover, at least 7.8% are prepared to take the most severe actions in the choices of answers in suing the service providers. This is found in the question on “share information without consent” variable (SSWC).

**[PF8]:** Getting treatment is more important than social embarrassment.

In the question of “Disclosure may result in Social Rejection (SDSR),” at least 73% of the respondents consider getting help in healing from the disease is far more important than social embarrassment and rejection

**[PF9]:** Even with a financial loss, half of the respondents will disclose private information to get treatment.

In the question of Disclosure may result in Financial Loss (SDFL), half of the respondents will disclose private information to get treatment.

However, at least 8.8% will not disclose to the provider but be cautious about their illness.

**[PF10]:** about 55% of patients will disclose the private information to the provider and complain about the breach or the staff (DWC)

In the variable DWC (Disclosure with Countermeasure), about 55% of patients will disclose the private information to the provider and complain about the breach or the staff. 12% will not trust the doctor to correct the problem and will change to another doctor.

**[PF11]:** When in an emergency, half of the respondents will disclose private information to the provider.

In the variable SDWE (Disclosure When in Emergency), at least half of the respondents will tell the service provider about their private information regardless of the condition of their sickness.

None of the respondents will risk their life by withholding private information in a life threatening condition.

[PF12]: 93% or patients will like to have control over their private data in EHR

In the variable SCDP (Control Data Privacy), at least 93% or patients will like to have control over their private data in EHR ranging from approximately 25% wanting to review their data; to at least 33.8% of the respondents revealed a strong intention to decide who can see the data by specifying a privacy profile.

#### **4.14 Chapter Summary**

This chapter provided the results of the survey from respondents who have been a patient within the last twelve months in Greater Toronto Area in Ontario, Canada. ANOVA technique is used to support the division of the three groups of respondents: (Online and Street, and Classroom group) into two population groups (Online + Street) and classroom).

Preliminary findings are observed with the discussion. An initial discussion of preliminary findings [PF] is identified to address research sub-question related to patients.

The detail data and result provided in this chapter forms preliminary findings on research sub-questions related to the patients. Such preliminary findings will contribute to the analysis and use triangulation design in converging preliminary findings to the research findings of this research study.

## **Chapter 5 Results of Focus Group Meetings with Providers**

### **5.1 Introduction**

This chapter provides the result of two focus group discussions as an instrument to study and to develop insights and themes from the providers' concerns related to privacy. The attitude of patients towards EHR is primarily influenced by their experience with service providers. Therefore, it is important to understand the viewpoints and practices of the providers to the patients. These discussions are also used as a triangulation confirmation of findings derived from the patients' attitude survey in Chapter Four.

This chapter is organized as follows: Section 5.2 describes the objectives of the focus group discussion. Section 5.3 outlines the methodology in conducting the two focus groups and data cleansing process. Section 5.4 presents the results of focus group 1: the nurses and pharmacists group with preliminary findings. Section 5.5 shows the results of focus group 2: the doctor's group. Section 5.6 provides observations and emerging theme from doctor's group. 5.7 gives the observations for other findings. Section 5.8 discuss the providers response towards the research finding. Section 5.9 provides a chapter summary linking Chapter Four, patient survey and Chapter Six key informant interviews with payers.

### **5.2 Using Focus Group Discussion with Service Provider**

The purpose of the EHR focus group discussion is to gather the perspectives of health providers (one support care group and one doctor group) to explore the



in-depth details of their viewpoints on the particular topics of privacy, its related risks and the concerns of the patients surrounding the EHR.

Grudens-Schuck *et al.*, (2004) compares the different methodologies between a survey method and a focus group discussion and reached the following assessments: “(1) Focus groups are used to explore the insights rather than the ability to generalize into rules as in a survey. (2) Focus groups extract information that is a combined local perspective rather than individual’s answers in a survey. (3) Focus groups members should have common attributes such as similar occupations, expertise or interests to ensure the quality of the information and (4) focus groups should have flexible conversations to assemble contents to insights rather than standardized questionnaire for fact gathering.”

In the discussion about EHR with service providers, the purposes of this research are to gain insights about their attitudes towards the privacy and perception of the patients and their concerns about using EHR in their practice. It is a qualitative theme and insight approach (Creswell, 2012) rather than a quantitative generalization. As the purpose of the discussion with providers is to understand how the attitude and practice of providers might provide a triangulation on the patient’s concerns observed in Chapter Four, the information extracted would be a local representation of the group participants rather than the answers from an individual person. This local representation is comprised of various medical professional groups: Group one is composed of nurses and pharmacists, group two consists of doctors from hospital emergency department and imaging departments. Some of the doctors also hold academic appointments, teaching at a local university. All these professionals are likely to have their ability to provide services impacted by an EHR.

### **5.3 Methodology in conducting the focus group discussion**

In ensuring the consistency and quality of data obtained in the two focus groups, the following processes were used.

#### **5.3.1 Enrollment**

In the context of this study, service providers that deliver health care to patients include two groups of providers. The doctors' group includes family doctors and hospital-based doctors that perform imaging, diagnosis, and treatment. Treatment and decisions are often needed urgently with severe illness or as a routine with nurses and doctors working in the emergency department. These doctors are Ontario licensed and have their practices in the Greater Toronto Area. The other focus group is the support group who are the nurses and pharmacists that provide services to patients by the orders of doctors. This study tries to find out if the completeness and accuracy of EHR information available would improve the quality treatment of patients significantly.

In ensuring the quality of data obtained from the discussion and the group-dynamic during the discussion, separate meetings with the respective groups were conducted to provide a maximum level of participation and a common base of knowledge and responsibilities in the provider job functions. The design of holding a different session for each of the two groups is based on the need to have a homogeneous group in the same profession. The objective of such design is to ensure that the group dynamics and perceived authority to express opinions is the same across all participants in the same focus group. It is believed that mixing the nurses and doctors in the same discussion will likely inhibit some of the nurses from freely expressing their views. Fern (2001, p.15) suggested that group cohesion promotes group dynamic and social status conditioned the personality of the participants in a focus group (Tresopakol, 2014, p.84)

The enrollment of nurses and pharmacists was through the selection of various organizations. This broad-based health care organization includes pharmacists from hospital and retail pharmacy. Nurses were enrolled from hospital ward and emergency departments as well as long-term care facilities. The physician's group were challenging to invite to participate in the focus group as they keep very busy, with tight and sometimes unpredictable work schedules. The author attempted to hand-deliver the focus group invitation letters, made phone calls and sent emails yielding very low uptake. A professional recruitment organization was finally enlisted and was successfully enrolled doctors for the focus group discussion. The above enrollment process conforms to an arm's length enrollment process.

### **5.3.2 Focus Group Settings and Data Processing**

Working towards the objectives of getting the contents of discussion in a social setting and observing the emotional feelings and reactions towards the topics from the participants, a formal boardroom with overhead videos camera and microphone facilities were used for the two focus group discussions. The author acted as the facilitator to solicit opinions and help consolidate the contents into common viewpoints. We used an instantaneous Delphi technique reflecting the contents of the discussion until a suitable consensus of the discussion point is reached. The observations of facial expressions and the intensity of the discussions were video recorded with agreement from participants in according to approved research protocols. For each focus group session, the camera recording facility was operated remotely in a separate studio outside the boardroom where the discussion took place. Therefore, participants have less awareness and are likely to have been a less affected bit the video recording.

Data recorded in videotapes for the session was first transcribed verbatim into written text. Relevant and essential contents were then examined and extracted into a spreadsheet using Microsoft Excel.

Data were then classified according to the topics of discussion from the original focus group planning guide. Sequences and reiterations of the same issue at the various time in the discussion was grouped, and insights were derived. The videotapes were also reviewed separately focusing on the facial expression and confidence level displayed by the participants when they expressed their points of view.

### **5.3.3 Professional requirements to protect patient's private information**

Professional licensing bodies have established legal guidelines and regulations for service providers to protect the sensitive nature and private information of patients.

#### For the nurses and pharmacists (in focus group one)

In this research regarding the service provider's practice, information privacy is used in the context of the ability of a person to control or influence the way in which his/her information is collected, used and disclosed. This definition is adopted from the collection of descriptions from the Personal Health Information Protection Act (PHIPA) 2004, Guideline to Personal Health Information Protection Act from the College of Nurses in Ontario and literature from information Privacy Commissioner of Ontario. The purpose of the PHIPA act is to provide comprehensive legislation to protect the collection and disclosure of personal health information about a patient.

Nurses have strict professional practice standards to keep patient information private. It is professional misconduct according to the Nursing Act 1991, if a nurse discloses without consent, information about a patient to a person other than the patient's authorized representative except when required by law (Ontario, 2009). The College of Pharmacists of Ontario also has clear guidelines issued by The National Association of Pharmacy Regulatory Authorities (NAPRA, 2009A, B) about protecting patient privacy when collecting and using relevant patient-level information. Preempted with these professional standards, the followings are the findings of the focus group discussion in patient privacy.

#### For the doctors (in focus group two)

In the area of protecting the patient privacy, the College of Physician and Surgeons of Ontario has issued strict guideline under policy statement #8 -05 (CPSO, 2006). It expects physicians and surgeons in Ontario to comply with the Medicine Act 1991 and the rules under the Personal Health Information Protection Act 2014. Specifically, doctors can only release patient health information under one of the following requirements. (1) They have expressed or implied consent from patients or a substitute decision maker. (2) They can release information when it is permitted under regulations of the College of physicians and surgeons. Such regulation included Regulated Health Professions Act 1991; Registrar's Investigations and Quality Assurance peer assessments (RHPA); or (3) it is required by law.

#### **5.4 Results of Focus Group One: Nurses and Pharmacists**

Together with the modulator (M), a group of five participants who are either nurses [N] or pharmacist [P].

The nurses work in a hospital or long-term geriatric care facility. Pharmacists work in a hospital pharmacy or a national pharmaceutical retail outlet. All of them have to work on patients' records in electronic form as part of their daily duties. All the participants in the group are in their middle age and have years of experience in their professions.

A pre-session document that included a brief introduction of the purpose of research with preliminary discussion questions was sent to the participants to help them think about the electronic health record in their practices. A semi-structured approach was conducted in the focus group meeting to study the topics of concern. The discussion followed the sequence of topics from patients' and providers' concerns on privacy; benefits; design and implementation; and concluded with a discussion on the operations and

practices of EHR privacy. The themes discussed will help understand some of the contributing factors that influence the service providers' (nurses and pharmacists) attitudes and subsequently influencing their practices relating to patient privacy. For focus group 1 with nurses and pharmacists, the following themes were discussed, and findings were explored. Some quotations on the discussion are given in the result below to enhance the depth of understandings.

#### **5.4.1 EHR benefits and risks**

Overall on the benefits from using EHR, the group agreed that there are many benefits in using EHR. However, the participants were concerned about the risks associated with the EHR information.

**[PF13]:** EHR has benefits but also has risks such as accuracy of information

One of the nurse-participants indicated that she would look forward to getting the EHR information otherwise a duplication testing would often need to be done. To emphasize the necessity of EHR, a pharmacist-participant expressed her concern that “who knows what they (patients) are on (medicine).” With EHR, she would have the ability to “actually look” at the medication history of the patient. This is important in her job to ensure prescription dispensed will not interact with other medicine the patient is having. While trusting the benefits of EHR, another nurse-participant is concerned with the accuracy of information as she has experience of incorrect data entered in EHR which “depends on who inputted it.” Further examination of the EHR benefits and potential risks show the following findings in the group’s practice

##### **(1) Increase efficiency and reduce error**

**[PF14]:** EHR will increase efficiency and make providers’ work easier

The group indicated that a prescription to pharmacists or doctors’ instructions to nurses is “easier to read” in an electronic form than the traditional handwritten format. The probability of misunderstanding a doctor’s order or prescription is now reduced, likely resulting in fewer adverse events and errors. With EHR

information, there would be a reduction in requiring patients to have a duplicate laboratory test such as “an MRI” would result to increase in efficiency and better healthcare quality. It will also be noticeable if patients are seeing many different doctors for the same illness. The health history in the EHR allows the group “to know” their patients better.

A pharmacist-participants substantiate on EHR has made her job easier that “the double doctoring is more for knowing the patient... “We have just started online less than a month ago with the narcotic monitoring system. So now if the patient’s got same drugs a month ago at a different location, it will tell us where they got it, the date they got it.”

**[PF15]: Reduce medical errors and improve quality of checking**

According to the members of the group, the interconnection of networks sharing EHR could make information more accessible to retrieve and share. This will enhance the quality of prescribing the drug if drug history or allergy warning can be obtained from EHR. The group also cautioned that while EHR information made available can increase time efficiency, it will also be their responsibility to confirm the information with the patient as a way of quality assurance and verification of information before treatment is provided.

Another benefit is on drug addiction, or the side effects of a newly prescribed drug might cause problems if information of concurrent drug used by the patient is not known. With an EHR, if a prescribed drug has been dispensed to the patient (even from another source), the EHR system would have captured detail information of the prescription. This helps pharmacists check and be aware of any effects when prescribing new drugs to a patient. Pharmacists also indicated that there are options to use a similar kind of drug (such as generic or brand name) to avoid any opposing medicines that the patient is currently taking if it is known via the contents of EHR.

In addition to a faster and better workflow when “physicians from various departments in hospital send the prescription electronically” the pharmacist-participants only need to dispense the drug, and the nurse can administer the drug with a well-labeled printout.”

## (2) Issues and Risks

There are other issues on EHR, but two are prominent one to the group are: Firstly, EHR is not yet fully implemented, and some modules have been delayed. Secondly, many of the group members are using either EMR or own organization's electronic health system that is non-standardized and non-interoperable with other systems. In the opinion of the author, as the delays have increased, new and better technology has become available.

[PF16]: Implementation is incomplete, still in transition, not connected Although some modules of the EHR are implemented, there are many other modules are still not fully implemented across the province of Ontario. One pharmacist-participant was apprehended that while "one module is online" but do not know when all the pharmacies will be connected." so that the drug history of the patient would not be incomplete.

[PF17]: Providers felt that it is time-consuming in inputting the EHR The group also has concerns that much time is now used in documenting the patient status and inputting to EHR records. Nurse-participants have indicated that this is time-consuming - inputting patient progress and information into the EHR. One nurse-participant revealed that "All the information, almost is the nurse that does the input- so we did a lot (and is time consuming)." The author has the experience of seeing a nurse almost spending half an hour in front of the computer to enter medical information about the progress of patients. This, in the opinion of the author, could potentially take away the time that this nurse is checking on and caring for the patient.

### **5.4.2 The Need and Protection of Patient's Private Information**

#### **(1) Information needed from patient to perform their work**

When asked with what critical information the group needs from EHR or electronic patient information that are in their system, the consensus includes the following. They are:



- (a) Patient-identifiable information is required in order to ensure that they are working with the right patient.
- (b) The need for any warning information that could be contradicting to their procedure at hand.
- (c) Clear information as to the correct type and dosage of drugs to be administered or dispensed to patient, and
- (d) Information to contact the person or a responsible representative when discharging a patient or to conduct a follow-up requirement when needed.

The group has discussed that although it is not mandatory, the ability to see patient's treatment history, allergy warnings and laboratory results can help nurses and pharmacists to confirm the correctness and quality of their care to the patients. This is especially important as one of their professional procedures is to double check for accuracy when providing treatments according to doctors' orders.

Pharmacists have indicated that they do not directly see the comprehensive electronic health records but could see the drug information sub-system in EHR such as the drug dispensary system. However, most of the electronic health information that they deal with is from within their organization – so possibly incomplete. Similarly, pharmacists in a hospital see some information from an electronic medical record (EMR) that is held within their hospital.

When asked what kind of patients' private information is necessary to perform their job, nurses felt that EHR (and EMR when they work in a hospital) helps them get a comprehensive picture of the patient's illness and symptoms,

The group confirms again that medication, diagnosis, and treatment information will be the critical information that they would like to obtain from EHR before they provide their part of the treatment. Imaging information would be a supplement and if available, can help them to establish a baseline of a patient's medical condition.

**[PF18]:** Critical information in EHR includes: Medication history, allergy warning, treatment history and drugs dispenses (taken) history in addition to the usual demographic information of the patient.

Nurse and Pharmacist on the discussion of critical information. The following shows an example of Delphi technique used in the focus group interview. [M] refers to modulator, [P] refers to the pharmacist and [N] refers to nurse.

[M] What is the information from EHR that are critical in order for you to perform your work correctly?

[P]: “I need the drug list and the past medical history, the two go hand in hand.”

[P]: “Nice to have (information in EHR) but I could do more grunt work- It just costs more (time). Well, I just ask the docs. – It’s just more grunt work. It does not give you (if the pharmacist does not get the requested information from a doctor). It’s not as good of a picture. If I knew their blood pressure in February was used to be fine, and four months later it is like sky high...you can build a really great picture from all this- when did this medication start. The patients aren’t very good with timelines, they are not very good with whom they say, who prescribed what, and you know, when they are discharged from the hospital, it is great to know there are a nurse and a dietician who looked after this patient... What can I do without? I guess immunizations, but it’s still...”

[N]: “See now, outpatient, we’re reviewing the patient; we have a list of patients before they come in. So quite often, we are looking at that list and preparing before we actually see the patient. So, the encounter history is nice to have before I even meet the patient, (From the EHR,) I need to know the treatments and what’s being done. Medication like for the Rheumatology clinic, they (nurses) need to know. For an orthopedic clinic- not so much. Moreover, the picture (this refers to diagnostics image), I am not so sure, and I know it is going to sound strange, but I am not so sure about the picture because the picture is only going to be accurate as the day it was taken. If it’s a year or two or so, people change.

[N]: “I think for me, I think medication, diagnosis, and alert (in EHR), like what kind of allergy-like penicillin is very important. But for like the address and the

telephone number, I think we should have a category, if I want to find it, we can find it...”

[M]: “I am also interested in not just the kind of the information such as the demographics... can you see a trade-off between types of medical information and ...the example that has been coming into use, let’s say, around mental health, somebody’s mental health condition is suffering from depression. Is there a category of medical information that you can say, well, I actually can do without that!”

[P]: ” There is always worst case scenarios. Let’s say that you (patient) don’t think the dentist need to know if you are depressed when they (dentists) are taking care of your teeth, and then they give you opioids, and now someone who had like maybe a really low time now has euphoria (a feeling or state of intense excitement and happiness) and spills into some kind of addiction, and that may have influenced the dentist for prescribing patterns when given the choices different drug. Moreover, you know you (dentist or pharmacist in consultation with the dentist) can use different depression drugs for different things.”

[M]: “In summary, in addition to the demographic information, is it true that medication history, allergy warnings, treatment history, a drug is taken are important to your job. Diagnostic imaging is good to have, but the value diminished quickly over time?”

[N]: “Yeah”

[P]: Nodded the head.

[N]: “Yes, that is why diagnosis (information/ history) is good to know.”

[P]: “Yes, but could do more grunt work (ask manually instead of from EHR)

[N]: “I think medication, diagnosis, and alert.”

## **(2) Protecting patient's private information**

### **(a) Deficiency of privacy protection**

When asked if there is a deficiency in protecting patient privacy in their working environment, both the nurses and pharmacists have indicated that many verbal exchanges of sensitive information were heard by others in the waiting room such as common private information that includes a telephone number, date of birth, home address and sometimes, medical history. There is no practice nor a particular room arrangement to protect overheard private conversations.

**[PF19]:** Verbal exchange of information can be overheard.

When asked about the protection of patient's privacy in their work environment, a nurse-participant expressed the concern that in registration or waiting room, many times that others can overhear conversation between nurse and patient regarding private information such as date of birth, phone number, home address and the patient's medical conditions in the waiting.

[N]: "The same what's true though is for outpatients, when you register, they go over your health care, your telephone (number). You almost have to be deaf if it's not to hear that information. So, I understand why people do not want to give anything". Pharmacist-participants confirmed that they have a similar situation when they have to explain to the patient the type of drug and the effect of it. Such conversation is easily overheard by others nearly.

### **(b) No full privacy protection**

**[PF20]:** No full patient's privacy

The group felt that there is no full privacy and indicated that some illnesses would be required to record in the EHR and be disclosed to appropriate government agencies. Such as diseases that normally carry a potential danger to the public. Therefore, full privacy is not something that a patient can expect.

[N]: "Yes, certain contagious disease needed to report." [N]: "(Knowing contagious disease from EHR) This will also work for our protection."

The discussion also clarified that when a patient signed a consent form to receive medical care or to be reimbursed the expenses by a private insurance company, the patient is actually “signs away their privacy. This allows the insurance company to obtain details about that particular patient’s care” Some part of the private information will be disclosed to third parties outside the circle of care (immediate care provider that are involved in treating the patient’s illness or medical condition). Very often, insurance companies have a good predictive model of the patient’s type and stage of illness by paying the cost of specific medicine that must be disclosed to the insurance company before the release of insurance benefits. The group further affirmed that patient should be aware that their level of privacy would be reduced when they sign a waiver form allowing healthcare administrator and insurance claim administer to access their private health information. There were discussions about whether a patient would pay out of pocket to avoid an insurance claim. The group has seen cases where such situation occurred. These incidents will be discussed in the section below on patients’ countermeasure.

**[PF21]:** Patients can have access to their part of EHR

When asked about the group’s opinion about patients’ rights to access EHR information, the group indicated that their professional standard and guidelines have a clear description that the service provider is simply a “custodian of patient’s information.” There are exceptions such as provider’s own notes belongs only to the service providers themselves.

Both pharmacist and nurse-participants acknowledge and agree that patient can access their part of EHR but would be in a paper format for “lab report to doctors” and imaging diagnostics such as MRI, ultrasound can be in electronic form by giving the patient a CD. One issue that pharmacist-participant reminded is that patient has to know how what and where to ask for their EHR information.

(c) Concerns of Unauthorized Access

**[PF22]:** There is an opportunity for unauthorized access to EHR information

When asked about the concern about unauthorized access to the EHR, the group has shown an uneasy feeling in that they worry more about illegal or third-party

access than the accuracy of information. They indicated that they have the standard practice of verification of the accuracy of information but are unable to know who could have accessed to see the data that they have entered. During the discussions, they have expressed concern about colleagues or regulatory bodies obtaining the part of data or notes that they entered into the system. The group understands that currently, many colleagues can access data of any patients in the system even though they are not directly assigned to the care of that patient. As long as they can log in and in a similar or a higher access role, they can see patient information. They also noted that there is a login trail should such misconduct take place.

A pharmacist-participant observed that in her work environment, another employee occasionally “came to the back (counter) and helped out with things. The pharmacist-participant also concerned about who is liable, the pharmacist or the worker.

One nurse-participant cited the extent of such exposure in that any “3000 employees” can potentially see the private information of the patient.

The group also discussed situations where a patient might have information overload. There were situations where patients obtained the drug information or treatment information and returned with worries and concern about the side effects or questioned the correctness of the performed procedure. It is understood that patient should be empowered with the ability to obtain more information on their illness. However, an overload of information and the patient’s ability to comprehend the information can be an issue. Although communicating and answering a patient’s question is part of the duties of a service provider, the fact that patient can now obtain a printed record of their health information, types of illness and status has facilitated some patients in looking up the information for themselves.

#### (d) Using lockbox concepts

From the literature review, the concept of “lockbox” provision in health information is a software control in EHR that can be an option available to patients when they make an explicit request to a healthcare provider to lock

specific private information resulting in the inability to release or disclose their specific personal health information.

“Clients also have the right to instruct that a part of their personal health information not be shared with other providers. This is referred to as the lockbox provision. If a client instructs a nurse not to release a part of his/her health information to another practitioner, the nurse must advise the practitioner that some relevant information has been withheld at the direction of the client” (CNO, 2009, p.6).

The same concept is stated in the policy statement issued by College of Physicians and Surgeons in Ontario to its members:

“The term “lockbox” applies to situations where the patient has expressly restricted his or her physician from disclosing specific personal health information to others — even to others involved in the patient’s circle of care.” (CONO, 2006, p. 3).

Some group members are aware of the requirements of the lockbox, but not all are believed in it.

**[PF23]:** Patient using lockbox may compromise the quality of treatment

When asked about the effect of patient’s requesting lockbox locking some of their private information, a pharmacist-participants indicated that with the locking of information, the provider also could not see the information which could “compromise the quality of care” to the patient.

The author recognized that there are various ways to implement the lockbox. Although Frelick, K. (2006) in her paper “Consent and PHIPA” has suggested compliance with the lockbox requirement by using (1) policies, procedure process (2) electronic or technical means or (3) combination of both (1) and (2). The group has a problem with using the electronic or technological methods to lock the information. The group indicated that they do not know of any technology provisions in their EHR system, nor there was any training to perform such a lockbox function to protect patient privacy in the EHR system.

Overall, in the area of privacy, the group has expressed the following vital concerns. Firstly, the group does not have full control of patient information as some information, and medical conditions must be recorded or reported in the EHR system. Secondly, the group cares about other medication that patient is concurrently taking. The EHR will help clarify any verbal answer from patients. Thirdly, there are still patients that exercised counter-measures rather than disclose private, sensitive information. Only a small number of patients will opt out of the system including disengaging from requesting treatment, paying out of pocket or seeking an alternative service provider. Fourthly, the group welcomes the modernization of recording patient's information using EHR, but their trust level in the EHR is still developing so the group is taking a "wait and see" attitude when more exposure and experience with EHR is attained. Finally, the group expressed that they are concerned about the privacy of their own-recorded information (data and medical notes) in the system.

### **(3) The error of EHR information**

[PF24]: Providers may make errors, EHR contains incorrect information

This data can be part of the EHR but will not be owned by the patient. The group acknowledged errors on some basic personal or private information could be spotted and corrected by the patient if they have access to their EHR.

Nevertheless, the chances of error are thought to be low. On the other hand, the patient will not usually have any skills and knowledge related to medical information residing in the EHR. The group indicated that when they spotted an error of the medical entry, they would often verify and simply correct the error. They emphasized that data errors are occasionally made, but their "working culture is to correct error rather than spending the time in tracking down" the 'who, what and why' the error was made unless a major consequence has occurred. Like many medical service providers, they are there to provide a service and their time is more valuable in spending with the treatment of patients rather than investigating a data error in EHR that has not caused a major adverse event or a near miss.



### **5.4.3 Patient Countermeasures to Service Provider's Need of Private Information**

#### **Provide incorrect information or being evasive in giving out information**

**[PF25]:** Patients withhold information or walk away

There have been situations where patients were either very reluctant to give out private information or simply walked away from the pharmacist when they were not comfortable in providing information such as address or medication history. It is hoped that EHR can have a better view of some demographic information of the patients by cross-checking various records and perhaps the patient will provide current contact information when it is essential for the provider to contact them.

The group also indicated that they have occasions where patients will try to be evasive or are not willing to provide the necessary information when providing their medical history. There were situations with patients worried about the protection of their private information and failed to disclose potentially relevant information. The group felt that the government has not sufficiently educated patients and the public that service provider needs some of their private information to enter into EHR.

The focus group has indicated is that sometimes, patients appear to hide information from them. There is the occasional encounter with patients who deliberately hide or give incorrect information.

[M]: "Have you had cases where patients do not want to give you some of the information?"

[P]: "Oh yeah we do. But not very often."

[N]: There are some people who don't give their (phone) number to us, they don't simply have one. They live on the streets; they don't have an address."

[P]: "Well, for my recollection, I mean, it happens, but you would have to explain that there are certain legal requirements for filling a prescription. You pretty much need an address, and if they don't want to provide it, I cannot fill their prescription for them. So, what I remember there're very short encounters

where they are unwilling, I may ask why you are unwilling because we don't even need your phone number. Like legally, all we need is their address."

[M]: "Do you have people (patients) who just walk away?"

[P]: "Yeah. Some people. Moreover, for some reason, if they don't want to give it, there tend to those who reluctantly give it, or they just walk away."

### **Hide information to avoid abuse**

**[PF26]:** Patient hides information to avoid an abusive spouse

When a patient provides incorrect information intentionally, it reduces the effectiveness of nurse and pharmacist's work. An example was that there were cases where patients were unwilling to provide their address because they were afraid to be "tracked down" by their abusive spouse or by authorities regarding alimony payments. The discussion also included information because of running away from an abusive spouse, financial trouble with creditors or people simply not wanting to be tracked.

### **Paid out of pocket expenses**

**[PF27]:** Patient paid out of pocket to protect privacy

Unlike most patients that wish to have their medical and drug bills paid by public or private insurance, there are the exceptions. One pharmacist-participant reported her experience that "I had with teenagers when they are on their parent's insurance plan, and they don't want to disturb (their parent) or something, they don't want their parents to know, they'll ask us not to put it on the insurance, and they will pay for it out of their pockets." From the author's view, this could be one type of many cases of patient paid out of pocket. Further research and examination of this finding could perhaps, yield some hidden issues that could be a simple administrative fix such as lockbox in EHR. The critical point is to assess and better understand the reasons for these paid out of pocket cases.

#### **5.4.4 Provider's Concern of own privacy**

Part of this research study is to explore if service providers have their own concerns about their data privacy in the EHR. A very engaged and lengthy discussion on this topic has occurred. The group expressed privacy concerns about their own data inputted by them and now resided in the EHR (or in their own organization's EMR or electronic drug dispensary system).

#### **Nurses concern about judgment from regulatory bodies**

[PF28]: Providers concern about the secondary use of information against them  
The nurses were concerned about government regulatory authorities or their professional licensing body in the access of the EHR information that they have placed in the record. Nurse-participants have all express varying degree of concern and uncomfortable feelings about the secondary use of EHR data to track their performance or mistakes. Example of such user of secondary data included "Government regulatory bodies, professional licensing bodies or their employers." One nurse-participant expressed that "if I want to be able to give the best possible care to the patient, I don't want to be thinking in the back of my head if I put this in (information to EHR), will somebody be coming to me later. I don't want to be thinking about that."

#### **Pharmacists do not overly concern about licensing body**

In contrast to the nurse concerns, pharmacists do not concern about licensing body reading information from their electronic records as they are used to be audited. They accepted and worked with the requirement that their professional licensing body "the right to come in and look through all your papers and hard copies." The pharmacist-participant took the attitude of the audit from licensing body as a means of issue identification and correction. To the nurse-participants, they felt that issues and problem could have been "picked up way before" the licensing body is looking through the EHR data. Another concern from a nurse-participant is that "it bothers me that the licensing body might have incorrect judgment as the licensing authority may be looking at a different context (such as incidents, performance) than the original intended context (such as efficient and quality care) when the nurse-participant entered the information in EHR.

### **The concern about sharing (proliferation) of nurse or pharmacist's notes or inputs to others**

There was a discussion about the judgment of one service provider may carry forward to another from information in the EHR. Therefore, hypothesis or suspicion of a specific medical condition might need extra attention and care before entering into the patient's EHR. The group has indicated that they would enter only facts into the EHR. The group felt that they do not have any immediate concern about researchers obtaining and working on sanitized (aggregated non-personally identifiable) information from EHR.

[P]: "I think this information (comments or notes in EHR) can be very subjective. The second you start saying things like you know it's not a difficult patient or any sort of analysis, you almost put a label on that person. Let's say me and patient X have a terrible rapport. Maybe I didn't make a fair judgment, and when they (the patients) go to see another provider, that provider is now going to carry that judgment forward. Moreover, I think it's almost unfair to patients to put (personal comments or non-medical assessment in the notes) in EHR. (If you put) all hard facts and I think you are less likely to get any sort of judgment."

### **Possibility of lawsuit**

When asked about the possibility of an increase in litigation, the group agreed that there is a higher chance for litigation when patients are given more information or able to access more of their health information in EHR. The patient can then discuss with other medical experts or lawyers and may launch a lawsuit against the hospital or the service provider. Such risk and potential of litigation are higher as patients learn to obtain access to their EHR, which is not current practice with paper records nor the hard copy of imaging photos.

**[PF29]:** Provider concerns about the increase of lawsuit

Nurse-participants have mentioned their concerns about a lawsuit on information that they place in EHR. Their countermeasure is that "when they entered their "notes" in EHR, they will think about how information might be perceived or audited. "It's not really like maybe the patient takes two Tylenol, maybe you have to write like 100mg Tylenol instead." One nurse-participant stated that there is concern from the hospital level about the giving out of

complete record to the patient and that some workers read everybody's notes. "I think it may increase lawsuit."

#### **5.4.5 Provider's Countermeasure of Concerns**

**[PF30]:** Providers devoting more time and carefully inputting EHR

Pharmacists may write information into the database in specific ways, like weight instead of the number of tablets, to prevent misinterpretation or to be used in litigation

They have indicated that "extra effort and time" is now spent in making sure the clarity of wording and pay much attention to the information entered as it is no longer in a paper form, but when in electronic form, the data can potentially be viewed by other agencies or government bodies. When entering sensitive private information of a patient, the group stated clearly that professional practices and ethics dictated that the benefits of the patient are to come first.

#### **5.4.6 Opinion on the Design EHR Related to Provider's Practice**

##### **Design**

The focus group was also asked to discuss and comment on their attitudes and perceptions about the design and their practice using EHR. They mentioned that while the design and functions of EHR system solve some issues but also created new issues with the use of new technology. This requires training for them on how the system should be used.

**[PF31]: EHR solves some but also creates new problems**

While EHR can increase efficiency from the use of information, it is time consuming when inputting the data as explained in the above discussions from nurse-participants. No longer will a pharmacist or nurse "misread" the physician's intention because what they type in for the prescription is what appears on their computer. A pharmacist-participant discover the "we have

never thought about you may log into the wrong patient's profile and start ordering a bunch of medication, which happens.”

When asked about trust and accountability, the group has expressed that perhaps the EHR should not be a top-down design (from Government to hospitals and providers) and implementation, especially as a government initiative. The feeling was that there are too many “fingers in the pie” with a government project. They have a “wait and see” attitude in their trust level on the EHR. They will re-evaluate their trust level once the EHR is fully implemented or their knowledge of EHR operations has increased. The group felt that strong traceability of logging “who” has sign-in, “when” the information was entered and the “what” information has been changed by the login person would help improve the accountability and gaining further trust as to the quality of information within an EHR.

**[PF32]:** EHR top-down design from Government does not get trust from providers.

A nurse-participant expressed her thought that when the government is leading the EHR project, it makes her “trust it a little bit less” because “there are so many things that get mixed and messed up and too many fingers in the (different) levels you know, things get mixed.”

### **Role-based design**

The group acknowledged that different roles and functions of service providers would need a different part of the EHR information. The role-based design in EHR is appropriate. However, when a service provider performs multiple roles or has their role change, changes in EHR access privileges will be required. This could slow down the health care efficiency during an emergency.

### **No or minimal training**

Many members of the group can learn to use EHR because they have experience in using an electronic health system.

It appears that there is little training in preparing the nurses and pharmacists in the use of the relevant part of the EHR module such as drug information module and imaging report module. There were discussions as to how much they can

trust the accuracy of EHR data. It is the consensus of the group to view EHR as an aid and it Summary of emerging them from Focus Group 1 (Nurses and Pharmacists)

The group agrees that more EHR information is better than less information. However, there is a feeling that they are not sure how to deal with the increased amount of available information. They emphasized that requirement and process of information depend on specific situations. It seems that at times, it is difficult to generalize the requirements and the process of using EHR.

The group still needs more experience in using EHR (or electronic health information) in their environment. They have a good understanding of the professional requirement of patient privacy. It is how they would enforce or comply with it under the EHR or their specific electronic health information system that remains a concern. Frequently, they expressed more of their concerns from a specific part of the EHR system rather than the complete system that is available as an information tool.

The group agreed that EHR will be the norm and will integrate the many electronic health information systems that are independently operated or not currently networked. Some of the focus group members' perspectives are based on educational or marketing materials from the government, and the group still seem to need experience in articulating or validating the benefits. The group reached a consensus that EHR is inevitable and thought that it would be a useful tool when fully implemented. It will be part of patient care.

The group seemed to focus more on their discussions on specific information that they are missing to do their jobs. With the moderator's focused question, they eventually discussed the impact of broader healthcare record that may contain information that they would have access to and how it would affect their work.

There was interest shown about how a comprehensive EHR information would matter at different degrees of importance in helping their job. Imaging information is essential to some nurses depending on the role of the task at that

time. The group has shown genuine concern for patient care and welcome information that would help in the efficacy of care provision.

The group felt that although they were quite clear as to the specific benefits in their immediate job responsibilities, there seems to be some vagueness in comprehending the more significant problem of privacy as it relates to EHR. The group liked the idea of the function of centralization of EHR records but has difficulty in understanding the distributed network topology. It is interesting to observe that the group's duality in separating their professional needs as opposed to their privacy needs when in the role of a patient.

Some members of the group were not comfortable with trusting the system. They have reservations about many aspects of technology, the integrity of information, the accuracy of information to the design and implementation by government agencies.

## **5.5 The Result of Focus Group Two: Doctors Group**

As Canada EHR implementation is defining the service providers (doctors and medical personnel) as the primary user of EHR, it is essential to explore the views of the doctors in focus group two in order to assess doctor's attitude towards the efficacy and privacy issues of EHR. Focus group 2 was composed of five doctors. These doctors work as a General Practitioner (GP), Radiologist (RD) and Internal Medicine specialist. The composition of focus group includes a radiologist, who performs diagnosis by viewing an image rather than seeing the patient. It is different from family and hospital internal medicine doctors who perform diagnosis and treatment prescription by examining the patient face-to-face. All members of this group have many years of experience in their profession.

It is an intentional arrangement to have focus group one with the nurse and pharmacists group held first to understand and to enlist some of their concerns on EHR. Focus group two with doctors can, therefore, be informed using



findings from focus group one. One of the objectives is to find out if doctors have concerns similar to nurses and pharmacists. For example, what are the attitudes of doctors in entering EHR information by recording sensitive patient information that can affect the insurance benefits of the patient?

Doctors are a group of busy professionals with a tight schedule and tight availability. Therefore, there was no pre-questionnaire to assist them in creating a baseline of the discussion. A list of topics was pre-defined to ensure that the focus group discussion is relevant in addition to some issues that are related to the findings obtained from Focus Group One (nurses and pharmacists). The following are areas of discussions and findings

#### **5.5.1 Benefits and Trade-Off of EHR**

The group has a positive attitude in accepting EHR. They have been using some form of electronic health information such as EMR, electronic health information system or patient information system within their organizations and practices. Their feeling is that EHR is far from its expected efficiency.

The group felt that they would rather have an electronic chart than a paper chart. They acknowledged that EHR is not a perfect record, but it is rich with health information. However, this is only useful if they can quickly find the information they need. The availability of comprehensive information will not have a significant impact on care for most routine cases. It will be helpful for complex cases. Sometimes, time is of the essence in their diagnosis and treatment of the patient. However, the attitude of the group is that with EHR, EMR or electronic health information system, the benefits outweigh the disadvantages. While some aspects of electronic record systems decrease efficiency such as time-consuming inputting and retrieving data, others increase it, such that the overall impression is that EHR or EMR is beneficial. Importantly, there is higher efficiency achieved in timely requests and receipt of patient charts and sometimes, critical health information.

### **Increase efficiency over paper record**

When asked if there is any trade-off in using digital information as compared to paper information, the group has indicated the following issues. It is more efficient to send digital information to specialists for consultation. In many cases, doctors are only able to receive information without the physical assessment of the patient in front of them. Doctors prefer EMR over paper records. The benefits outweigh the disadvantages. While some aspects of EMR decrease efficiency, others increase it such that the overall impression is that EMR is beneficial. Importantly, EMR increases timely requests and receipt of patient charts.

In the next potential finding, it shows a quick Delphi technique to obtain a consensus of finding. The following legends apply: [M]= Modulator;

[HD]= Hospital Doctor; GP = General Practitioner, [RD] = Radiology Doctor

**[PF33]:** It is better to have electronic chart than the paper chart, EHR not perfect, but rich in information.

The EHR is not perfect but is rich in information.

[RD]: “Would still rather have an electronic chart than a paper chart any time of the day. If I have to request paper charts, it might take another day and take a much longer time.”

[GP]: “Yes, I agree.”

[HD]: “It’s not a perfect record, but there are many data if you know where to look (from diff physicians, biopsy results).”

[M]: “So, do we agree that electronic chart is better than paper chart even though EHR is rich in information?”

All participants either verbally or nodded to agree.

On the positive side, the group mentioned that the administrative chore and sometimes frustration in getting a paper copy (fax copy) of health information could be vastly improved with the use of electronic records.

## **Digitization of Information**

The group also indicated that when information is in electronic form, it might be useful for patients to be able to log into a console provided by the hospital and see the information, such as referral letters before they are sent out. If information has to be sent by mail, there could be multiple addresses and that the privacy of patient might not be protected. The providers cannot ensure who is opening the email. In case of electronic access to EHR or EMR, the patients themselves can access the information. Urgent information can be shared much more rapidly if the data is held in a digital format and updated in real time.

The author has seen patient sign-in/information system is implemented in some hospital, such as SunnyBrooke Hospital in North York region and Princess Margaret Hospital in Toronto.

The importance of timely transmission of information and availability of comprehensive data across different medical specialties confers benefits. The trade-offs are potential challenges in spotting and correcting errors in electronic records. The group thinks that improvements could be made in EHR, such as allowing patients to log into their records. This could ensure the accuracy of information available and ensure delivery of information to the patient is private.

[RD]: “(There are laboratory EHR available) It is useful for patients to be able to log in and see info (like referral letters) before they are sent out. If things are mailed to the patients’ address, (a) there could be multiple addresses; (b) cannot ensure who is opening the letter (decreases privacy) if (they) have electronic access, the patient themselves can access the info.”

[HD]: “And patients can sign up for it, and access imaging/lab results. This is a two-way thing with patients/physicians being able to access the information. Physicians should be able to decide which (referral) letters are available.”

[RD]: “Therefore it becomes patients’ responsibility, not just doctors.”

### **Patient access to information**

Doctors think that it would be a good idea to have patients access their laboratory results and perhaps some imaging records. Their opinion is that patient would be interested in seeing their test result. The group suggested that the choice of which item in the laboratory test is to be available to the patient should be decided by the doctors.

The author noted that since the patient owns their medical information and doctor is only the custodian, with a patient having the capability to see and print copy of their record, it would save the administrative task of making photocopies of the result when a patient is asking for it. Under the law, patients have the rights to ask for a copy of their medical information resided in their doctor's facility.

According to the discussion in the group, there are methods currently in place to reduce misinterpretation by patients from doctors' referral letters. These are not affected by whether the delivery of information is written on paper or digitalized format.

When asked if patients would be confused and misinterpret the laboratory results or medical information that they are entitled to have and obtained it from doctors, the group felt that there are ways to reduce such situations. This includes discussing with the patient about the medical information before the patient can obtain it. There is need to avoid ambiguous terms in the medical record. The author noted the practice from Laboratory that patient results will only be delivered to doctor. Therefore, patients can only see and obtain a copy of their result when in discussion with the doctor.

One concern raised is that they found that with much information and database available, it takes time for them to navigate or find the information that they need. They have observed nurses spending a substantial amount of time in typing detailed health information into the electronic systems which could eventually part of the EHR system. While this should improve the quality of clinical information available, it comes at the cost of nurses spending less time providing care to patients. The viewpoint is the quality of the actions. If

spending the time with the patient is of a higher quality and necessity than EHR, they should do so or vice versa if the timely inputting of health information is necessary to yield a better diagnosis.

**[PF34]:** Information hard to find, perhaps due to a lack of training.

One hospital doctor-participant explained that accessing EHR “is time-consuming and I have a case where it takes two hours to find information with this new technology.” It was later found that it was “an issue if can go into another database but don’t know how to read it properly.”. The author interpreted this, perhaps a lack of training for the service provider in using the newly implemented EHR system.

## **5.5.2 The Need and Protection of Patient Private Information**

### **Information needed from patient to perform their work**

The group was asked to enlist the critical information that is important in their practice to perform diagnosis or treatment of the patient. They stated that information on previous medical treatment, laboratory imaging, and previous surgery would be critical to their practices during the diagnosis stage. When considering the treatment with a prescription, they will be looking for a patient’s medication history, allergy and response to previous treatment. Any missing, incomplete or outdated information from EHR can quickly be obtained from the physical examination of the patient.

**[PF35]:** Doctors need medical history, medication history and treatment history

A hospital doctor-participant expanded on the needs using an example as the need to know “when chemo/radiation therapy was conducted. Some like surgery are nice to know, but some like medication and imaging are important.” On the other hand, radiologist-doctor participant claimed that image for “timely diagnosis” is important, “not just the written word” in EHR data.

### **Patient Privacy in EHR:**

The group agreed that there is the need to respect and comply with protecting the privacy of patient information in EHR. As the primary role of doctors is to perform diagnosis and determine treatments for patients, their focus in their work is to obtain the necessary information from patients, from laboratory results and their examination of the physical conditions of the patient.

Therefore, the recording of the patient's diagnosis and treatment information in a private manner in EHR becomes a critical undertaking. The purpose of guarding the privacy is to prevent adverse impacts on the patients from third parties such as insurance or even family members.

**[PF36]:** Doctor uses own private code to protect patient privacy

The practice of protecting patient privacy is used in various forms. One very efficient way doctors use it is to encrypt patient's private information or medical observations and doctor's notes by using doctor's private codes. [HD]:

"Suspected origins of conditions may not be written; e.g., Loss of nasal septum is often caused by cocaine use, but this case would not be written out without actual proof, so will use my own private code only understood by myself" If information is in plain language, might otherwise have impacts on patient's insurance benefits. [HD]: "Patients have questionable conditions (hypertrophic cardiomyopathy, HCM), we have to be careful what to call it on the record because it affects insurance if they apply for insurance.

Unlike the nurses or pharmacists group, doctors are less concerned about the address and identity of the patient. The private information that they are concerned with in the EHR is suspected medical condition that has not been thoroughly tested with the confirmed result but could label a patient in the view of another user of EHR or an insurance company.

### **The error of EMR / EHR information**

EMR is the electronic health records that mostly centered on an Institute basis, such as a hospital or a clinic. It is amalgamated to be part of the more extensive information system of EHR. Most doctors dictate their medical notes and diagnosis using the electronic audio recorder in their practices for time-saving

between seeing patients. Instead of coding certain words in the EHR, doctors may leave incomplete information out of the referral letters or records entirely. Of the group of doctors participated in discussion 60% use voice transcription software and 40% use other people to transcribe their case-notes. Both voice transcription software and human transcription are methods used to transcribe information dictated by doctors. Almost all doctors have a dictation process. The group pointed out that electronic transcription software may be more error-prone than human transcription. Although labor is saved when using electronic software, the accuracy can be worse, and therefore the efficiency of the transcription could be an issue. When there is suspected error in information found in EHR or EMR, the doctor will review it and may simply reassess the patient. Very often, it is considered a difference of opinion from another doctor.

The group was asked if there have been situations where records in the EHR do not match the identity of the patient. The group confirmed that there are cases where the EHR/EMR information was not accurate. For example, there were incorrect numbers entered during dictation (e.g., session number) or an incorrect addendum added to the report. Such errors are not always easy to detect. This is because a record stored in the system can be in different formats (e.g., notes, charts, and images) and can get very complicated to assemble into a screen view when it is being accessed. Another issue is that information can frequently be updated by many other service providers. The group also claimed that the EHR error had not reached the level where entire identity has been switched (wrong record). It is generally some minor errors in accuracy has occurred in the system. All service providers, especially nurses and administrators should double check information before releasing it into the computer or the hands of other providers.

The group indicated that mistakes are not necessarily recognized, as it could be interpreted as a difference of opinion from another doctor or possibly that the patient's condition has changed. The incorrect information may still be misinterpreted in the future when it is held in the EHR system. In such case, information in the electronic record may be counterproductive because later diagnoses may be contradictive of previous diagnoses. In medical records, data are not necessarily retroactively fixed. When correction becomes mandatory, the

original document is altered with a clear trail of what has been changed, and the information of previous outdated record will be archived for future audit if necessary.

**[PF37]:** Doctors see errors in EMR/EHR, but not of significant impact

When asked if doctors have seen EHR record does not match the patient, and where it might be a wrong record, one HD-participant sited that “Sometimes the wrong number entered during dictation and it might not be obvious.” Another HD-participant also mentioned the fact that “Info can get propagated through years, even if it is wrong. However, still, use EMR? Yes. Because work with community partners and it can be frustrating if the info does not transmit between systems.” The participants also explained that (if in doubt, correct) “information could get through phone or fax.”

### **5.5.3 Patient Countermeasures to Service Provider**

#### **Patient withhold information**

**[PF38]:** Doctor observed that patient withholding information is rare, but might occurs when with family members

When asked if there is any deficiency in performing their duties if patients withheld information to them, the group has confirmed that there are such cases and deficiencies do occur. They have observed that such withholding of information happened more often when the patient is with their family member than just the patient alone with the doctor. GP-participant: “When Medication or substance (is)use, (it becomes very) dynamic within the family. Often, see family unit (patient & family) together, patients will provide difference info that they may not want to be shared with other family members.” For the radiologist doctors who do not see patients personally, they read the image and make a diagnosis based on images taken by technicians; their concern would be the accuracy and completeness of information in EHR. The group also indicated that they have other means to detect and verify the missing private information. This is especially so when the patient is available to them for



further diagnosis. They indicated that efficiency would be reduced if missing information in EHR were not updated. In their experience and opinion, the group claimed that patient's withholding information to them is rare especially when there is no other family member with them. The group is optimistic that they will be able to detect any illness related information based on their examination of the patient themselves and that they have a process to verify patients claims and descriptions of their symptoms as part of their diagnosis procedure since they can always perform another checkup in the examination room.

In the discussion of the potential reasons for patients not to disclose complete information to doctor, the group indicated that some of such behavior is related to patients' insurance benefits. The group understood that some of their diagnosis information written in the EHR might cause the patient to have a reduction or disqualification of their insurance benefits. The group discussed situations with some of their older patients who are retired. These patients either have out of pocket insurance coverage or have no extra insurance coverage at all, other than their basic government OHIP (Ontario Health Insurance Plan) which does not cover most prescription medicines. When appropriate, doctors would normally assist the patient to maintain their insurance benefits by issuing prescribed medicine and withholding diagnosis information on not yet confirmed (but suspected) course of the illness. For example, there were cases where a doctor treated the symptoms of a patient, under cross-checking of such symptoms with other physical examination; it would lead to an underlying suspicion of occasional drug use. The doctor may decide to treat the symptoms of common illness and not write the suspicions in the EHR. This is especially so when there is no further tests or facts to support such suspicions. Alternatively, the doctors may code the suspicious cause in the doctor's notes with a private code that only they would know the meaning.

**[PF39]: Patient withhold information fearing the loss of benefits**

When asked if the patient would withdraw private information if there is a potential loss of their benefits, doctors replied that they are trained and are sensitive to patients' needs and requirements. This is especially so when a

financial benefit is at stake. In some cases, when they assessed that patient might have certain “suspected medical conditions,” they will be cautious in writing the information in EHR as they know that the information may “affect patients’ insurance benefit.” RD-participant also reminded every one of the fact that insurance company can ask for medical records when a patient “give consent” in their insurance claim. Therefore, “it is unavoidable that insurance companies see patient records.” Another HD-participant viewed that insurance company sometimes uses the medical information (from EHR or Doctors) to the disadvantage of the patient and in some case it (the decision is “rather arbitrary.”

#### **5.5.4 Providers’ Concern of Their Privacy**

##### **The concern of litigation to providers or their hospital**

**[PF40]:** EHR may expose doctors for prosecution

When asked if the group has concerns about their private information being entered into the EHR system or electronic health system (EMR), most have expressed that they have some level of concern and there was a discussion on how they would design ways to protect their private information. There seems to be a concern to protect themselves from potential legal issues or being sued for medical malpractices. Digital information can be shared easily, and the exposure of such information to a broader audience than paper record created concerns for the group.

Similar to the concern from the nurse-participants in that someone reviewing or reading the EHR may be using a different context (different purpose) than the context of the doctor who entered the information to EHR. One HD-participant has revealed that “I have a colleague who was sued because diagnosed was not done in a “timely manner.” Much valuable work is not recorded in the system, such as consultations”.

The group claimed that they use the same technique to protect their private information by coding (own secret code) the information as they have done so to protect the patient’s private information. Different medical specialties deal

with varying degrees of sensitivity of doctor's private notes or patient's private information. Doctors do not wish to be accused, sued or disciplined for indicating sensitive private information in plain language on the record. However, they like to remind themselves to follow up on specific observations or suspicions when they see the patient again. For example, when issuing a referral letter for a test for parents such as for genetic tests, the doctor would need to be careful about the reason for the request. They will write their reasons in their notes with own private code but will not give it in the prescription or referral letters.

There was another example of suspected origins of conditions that may not be written in the EHR. For example, a loss of nasal septum is often caused by cocaine use. Such a case would not be written out without actual proof or further test. For the legal protection of the doctor, this kind of private information before confirmation from a laboratory test. This information will not be written in the patient EHR as it could implicate the patient (e.g., for substance use).

Also, patients that are asking for the records or request to see the record in their office is also a concern. Patients might be able to learn of whether a doctor is suspicious of their substance abuse, for example, by getting a copy of their EHR information. According to the group, if medical suspicions written by a doctor are incorrect, then the doctor, in the worst-case scenario, might have to face potential litigation.

The group felt that most providers' information on patients could not be hidden away in an EHR system. Before the confirmation of the suspicious substance abuse, for example, the doctor might not provide full information. At some point in time, during the treatment of the patient, this private information would be disclosed once the diagnosis is confirmed. Such disclosure of the information would be available to other health care professionals or regulatory bodies or insurance companies. In the area of incorrect information in EHR, [HD]: "If (doctor) notices cases of negligence, (they) will not say that another doctor was (has made a mistake). May just say he reassessed the information (differently).

The author observed that both the nurse group and the doctor group have the culture of not trying to investigate the source of Error of EHR data (section 5.5.2), but to fix the data and merely move on.

#### **Using EHR for another purpose: Benchmarking a doctor's productivity**

**[PF41]:** Providers concern of using EHR to evaluate productivity

When asked about the secondary or administrative use of the EHR (EMR) information resided in the system such as used by their employer or regulatory bodies to evaluate the doctor's productivity, the group indicated that they do not have much concern about such use. The group felt that their work performance under EHR tracking is not a significant concern. It would not be good to use an electronic system to measure their performance. However, the group felt that their primary concerns are the curing of the patient and their performance should be a measure of their work with the patient rather than from an EHR or any patient information system.

The group is aware that government might get access to data regarding the productivity of hospitals and even of individuals. Some group members indicated that the information of their productivity regarding responsiveness in taking care of the patient is already available from the paper system. However, EHR makes the collection and analysis of data much easier and faster. Another perspective from the group is that they are not concerned about sharing information at the institutional level, but they have concerns if others are looking at their part of the information and misunderstand the information or use a different performance criterion for comparison of their work.

#### **5.5.5 Providers' Countermeasure of Concerns**

**[PF42]:** Doctors code to protect their own sensitive and private information

##### **Coding of private information**

Due to sensitive nature of the patient's private information, especially in an electronic form, doctors need to find a way to code information such that they can still understand it when they go back to the same record, whereas a third

person such as insurance administrator or legal investigator may not understand it.

The coding of information in doctor's note and EHR is to protect the patient's benefits and the privacy of the doctor in their assessing of suspicious but not necessary confirm illness of the patient. Very often, this suspected illness is not part of the immediate condition to be treated. Doctors will code their notes to protect the patients and sometimes their observations when this unrelated illness is not part of the immediate illness of the patient under treatment. The group intends not to write the suspicious activities (such as substance abuse) in their record, as this may cause the denial of an insurance claim by the patient when such information is not confirmed with the diagnoses. The group indicated that they needed to learn how to code and transcribe information from noting the symptoms of a particular disorder so that they can remember what it is next time they see the record. They believe that when a diagnosis has not been made, then the insurance company cannot deny or reduce patient's benefits. With their private code in the record, the doctor can be reminded of what to look out for next time when they see the patient. This is contradictory to the intent of an EHR that is to be shared, but information is purposely coded in a doctor's note that only the same doctor who wrote the code knows what it means.

### **Doctors' notes and dictations**

When asked if the group keeps separate data and information that they do not wish to place in the EHR, the group indicated that they use doctor notes and voice dictation as a form of recording their findings. When dealing with private patient information that is pertinent to the protection of the patient or in some cases, protection for themselves, they will find ways to create a unique code that only they can understand when combining with other information placed in the record. When transferring handwritten notes from paper charts to dictation, just certain information would be transferred, and the remaining information can be kept private. Patients only own the information about themselves that from their laboratory test and they have access to the given prescription that relates to their illness. Doctors' comments and notes belong to the doctors, as they are the originator of such information. Some other group members indicated that most

of the time, they would write nearly everything, but occasionally substitute words for private and sensitive information that they consider as important.

### **5.5.6 Efficiency and Design of EHR**

**[PF43]:** EHRs are not organized, hard to find and time-consuming to get the right information

The attitude of the group is that EHR can be better organized. In their opinion, it is inefficient and slow to find the necessary information. It appears that navigation in EHR to get the information they need is not easy or intuitive. The group has suggested that the capability to customize the screen and presentation of information would be helpful in their daily work. There was assertion from the group that user interface is not intuitive and that they would like to see more pilot tests first at doctors' offices before finalization of the interface.

**[RD]:** "There is no way to customize UI (User Interface) nor choose units in the interface; I like to be able to see tests (done) by other doctors."

### **5.5.7 Security protection and Cybercrime**

**[PF44]:** Information Security protection is the responsibility of the Government. Cybercrime needs legislation

The group of doctors believes that it is the job of the designer and implementer (payer) of EHR to ensure high-security protection and to prevent unauthorized access to EHR. Hospitals and medical clinics already have security procedures to protect patient information on their local computer facilitates. The extract of different databases and servers across a communication network to form the EHR requires security protection by design and proper implementation.

**[HD]:** "Sometimes patients worry about things far less than the practitioners though; e.g., patients will ask for records through email, but practitioners cannot do that because it is not a secure mode of transportation. However, some patients do not care; they want their referral letter (in an email)".

The protection using information security and prevention of cybercrime should be part of the design and implementation of EHR system. In their opinion, legislation is always behind actual practice. Legislation can help at the macro levels but perhaps is not very helpful at a micro patient record level. Many times, legislation is a result of a pattern of computer incidents or security breaches. There is a concern with the transmission of EHR information from across the computer network.

There was a discussion about doctors in the US using wireless devices within the hospital to access patient's data, and in some cases, their handheld devices can receive the medical information from patient's monitoring system.

[HD]: "Patients that aren't that concerned will disclose info, but paranoid patients will never even ask for the record; so, the number of patients who seem like they care (about information security) may not even be accurate."

#### **5.5.8 Computers and doctor-patient interaction**

Increased use of information technology in medical practice changes the way in which patients and doctors interact. Patients can feel that they are being ignored as the doctor spending insufficient time in examining them. When asked about this, the group responded that during the examination of the patient, they would seldom use computers to access the EHR records. They will do it before or after seeing the patient. Some doctor will use the computer in front of the patient but will limit the time in such a way that it does not interfere with the discussion and relationship with the patient.

#### **5.5.9 EHR implementation – how to make it successful?**

The group commented that EHR/EMR aims to improve quality of care. It solved some of the current problems in health care delivery but created new ones as well. Other countries have failed in implementing large ehealth projects, such as imaging networks. It is noted that the intentions of EHR program are good, but the implementation of EHR initiative needs many improvements. In other countries, there has been the successful implementation

of EHR where information and implementation come from the local medical community. Standardization across the province or country takes away customizability.

Questions were asked if EHR should be created starting from a group of medical organizations (community) at the initial stage. The group came to the consensus that it would be better to start with a small medical community. The idea is to conduct comprehensive design and improvement with pilot implementation to see how well the design and implementation work with system objectives and standard practice. After this has been achieved, then move on to increase the expansion to other medical communities with duplication of standards and customization of local usage. Many decisions should be made at a low level, not at a policy level. This is a bottom-up approach to design and implementation.

In the author's opinion, there is both the need to define the standard at a national level and implementation at the local level. The emphasis is that local level of EHR implementation should be, by design, fit into the national standard level for across the province and nation compatibility and sharing of records. When a local system has already been proven with EHR functionality and benefits, it may be easier to retrofit the system interface to the provincial or national network instead of abandoning the legacy system and build a new one.

It was also suggested that there should be the layered accessibility of information at a department or institute level in addition to the current role-based level assigned to medical practitioners.

The group suggests that the design of EHR should be bottom-up from regional or local users. It will then have the most acceptance of the system, as it will address the requirement of the regional user or local hospital. The system should then be interconnected with different interfaces to form a more substantial and workable system. This will ensure that as the system has increased coverage and it does not sacrifice the requirement of local users who are the primary and most frequent users of the system. The group has cited various local electronic health information system and EMR systems that were successfully designed and had higher acceptance.



The group understood that EHR is a national initiative and standardization and interoperability is a prime requirement of the project. The group questioned that if EHR is not fully utilized and other local systems are not integrated to EHR, then there will be duplication and the funding and maintenance of EHR systems will result in substantial costs, thus offsetting one of the original objectives of the EHR system.

The group suggests that for the EHR system to be useful, it has to have sufficient transparency to gain trust and accuracy. It requires government legislation to ensure that information used is within the purpose of design, and any adverse impacts should be minimized especially the use of new digital technology. Although many hospitals and clinics have some form of EMR and electronic health information system, the establishment of new modules such as imaging modules or a drug information module could duplicate some of the existing systems. This requires attrition or adoption of an interface with a current system that may be not fully compatible with EHR. The group suggests within the design of the EHR; there should be ways for a physician to encrypt specific private information.

There was also view made that the new EHR system can be easily installed in rural areas where there is no competing electronic health system available. In some hospitals in Toronto, there were hand-written records still in use. There was no plan to transform handwritten information into digital information that can be used in EHR. The point is that the use of EHR will be better and higher coverage may be achieved in future, as hand-written records were not easily integrated into the current system. Therefore, the objectives of having complete and comprehensive records are limited which results in less efficacy of EHR.

**[PF45]:** Interoperability has not been extended to most hospitals

Regarding interoperability, the group claimed that many health provider organizations such as hospitals, clinics, and laboratories are not interconnected using the EHR network. They are still using localized EMR. Health information networks in their hospitals are mostly not connected to other systems. Special arrangements must be made to send electronic information to another hospital or other users. There is the trend of increasing inter-connections to partner or

affiliated hospital, but the process is far from optimal. Connecting to the EHR system is still a module-by-module process with some modules still incomplete.

## **5.6 Observations and Emerging Themes from Group Two (doctors)**

Doctors engaged in the discussion at a management level in addition to the practice level. They are concerned with the design of the EHR and made suggestions as to how to implement a successful EHR. The discussion invokes the use of theory and models during their critical thinking and analysis of the questions asked. In comparison with focus group one (nurses and pharmacists), focus group two (doctors) seems to have less technical and administrative training in the use of EHR and as such that it takes them more time to find the right information. There were different opinions expressed among members, but in many cases, the diverse views and differences came to some form of consensus.

The group thinks that, although the purposes and intentions in the design of the EHR are right, the top-down implementation may not work as effectively as a bottom-up implementation. In the group's opinion, this approach can be achieved by small successes first in a bottom-up model, then expanding the medical community into a broader region and so on. Multi-layered systems regarding accessibility may solve some problems; however, it makes the system very complicated. There was no clear consensus on how best to achieve success. In the area of protection of patients and the doctor's privacy, doctors indicated that they use private codes to replace sensitive information to prevent the third party from seeing the information.

Doctors rely on government legislation and enforcement to ensure that cybercrime is prevented. They understand that information in an EMR/EHR does not provide the complete data necessary to make a diagnosis and treatment plan. Patients and third parties may misinterpret this information in EHR.

There is a trade-off between the convenience of data accessibility and security in protecting the privacy of the patients and the privacy of doctor's notes and information. Doctor perceptions of patient privacy may also be skewed because patients who are concerned with their privacy may not see a local doctor in the first place. Interoperability is one of the core requirement of EHR, aided by uniform data collection and common export formats. However, there is the little capability to allow doctors customization of their computer screen and information within the EHR. Patients will adapt to technological integration, such as the notion of doctors using computers during the examination. Currently, most doctors (based on the focus group) do not use the computers during patient encounters only using a computer before and after seeing a patient. The discussion of this aspect perhaps is too early in the implementation stage. Currently, there is no concern that computer use will hinder patient-doctor interaction.

## **5.7 Other Observed Preliminary Findings**

**[PF18]:** Nurse and Pharmacist on critical information include: medication history, allergy warning, treatment history and drugs taken history in addition to the usual demographic information of the patient

**[PF35]:** Doctors need medical history, medication history and treatment history

**[PF20]:** No full patient's privacy

**[PF19]:** Verbal exchange of information can be overheard

**[PF25]:** Patient withhold information or walk away

**[PF26]:** Hide information to avoid an abusive spouse

**[PF27]:** Patient paid out of pocket to protect privacy

**[PF33]:** It is better to have electronic chart than the paper chart.

**[PF36]:** Doctor uses own private code to protect patient privacy

**[PF37]:** Doctors see some errors in EMR/EHR, but not of significant impact

**[PF38]:** Patient withholding information is rare, but might occurs when with family members

**[PF41]:** Concerns on using EHR to evaluate productivity

**[PF42]:** Doctors code to protect their own sensitive and private information

**[PF44]:** Information Security protection by Government, Cybercrime needs legislation

**[PF45]:** Interoperability has not been extended to most hospitals

## **5.8 Preliminary Findings on providers' response towards the research questions**

Iteratively, the following preliminary findings[PF] are related to the items listed below within each research sub-question. These PF will be triangulated and review and analyzed in Chapter 7.

The two research sub-questions identified in Section 2.7.1 are

*(Q7): What are providers concerns on EHRs systems?*

(a) Deficiency of privacy protection

**[PF19]:** Verbal exchange of information can be overheard.

(b) The opportunity for unauthorized access

**[PF22]:** There is an opportunity for unauthorized access to EHR information.

(c) A patient using lockbox may compromise treatment as information is not available.

**[PF23]:** Patient using lockbox may compromise the quality of treatment

(d) The error of EHR information

**[PF13]:** EHR has benefits but also has risks such as accuracy of information

- [PF24]:** Providers may make errors, and EHR will contain incorrect information
- (e) Solves some problems but also creates others. The related PF are:
- [PF14]:** EHR will increase efficiency and makes providers' work easier
- [PF15]:** Reduce medical errors and improve quality of checking
- [PF21]:** Patients can have access to their part of EHR
- [PF31]:** EHR solves some but also creates new problems
- (f) Records not organized, input and retrieval of records can be time-consuming, and providers need training. The related PF are:
- [PF17]:** Providers felt that inputting the EHR was time-consuming
- [PF30]:** Devoting more time and carefully inputting EHR
- [PF34]:** Information is hard to find, perhaps due to lack of training
- [PF43]:** Records are not organized, hard to find and time-consuming to get the right information
- (g) Top-down design not trusted by providers
- [PF32]:** EHR top-down design from Government does not get trust from providers.
- (h) Benefits are limited by incomplete implementation
- [PF16]:** Implementation is incomplete, still in transition, not connected
- (i) Opportunity for unauthorized access
- [PF22]:** There is an opportunity for unauthorized access to EHR information
- (j) A patient using lockbox may compromise treatment as information is not available.
- [PF23]:** Patient using lockbox may compromise the quality of treatment

(Q8): *Do providers have privacy concerns in EHRs as they also placed their personal identifiable information, diagnosis, and notes in the EHRs?*

- (a) Concerns about the secondary use of information to judge providers

[PF28]: Concerns about the secondary use of information against providers

[PF41]: Concerns on using EHR to evaluate the performance

- (b) The concern of litigation to providers or their hospital

[PF29]: Provider concerns about the increase of lawsuit

[PF40]: EHR may expose doctors for litigation

## 5.9 Chapter Summary

This chapter focuses on the expert discussion and consensus from health service provider. Two focus groups (nurses with pharmacists and medical doctors) were conducted to achieve maximum and free-flow participation and group dynamics by gathering groups in similar roles in using EHR. Some of the questions were asked based on a further exploration of some findings from Chapter Four. The answers from focus groups provide opinions and data for further triangulation of the EHR initiative both from patient's attitude and the payer's implementation. In the next chapter, eight separate key informant interviews with key policymakers, medical association executives and lawyers are described to understand the viewpoints and constraints with the design and implementation of EHR.

## **Chapter 6 Results of Key Information Interviews with Payers**

### **6.1 Introduction**

This chapter discusses the result of eight key informant interviews. Participating key informants were subject matter experts in their EHR related street. They were the senior managers or executives in their organizations, which directly involved in the development and implementation of the EHR program group or professional bodies that were key stakeholders of the EHR project.

In increasing the trustworthiness, credibility, and validity of the collected data for further analyses and understanding of the efficiency and efficacy of EHR, a qualitative triangulation methodology was used to obtain multiple data sources from various persons and different organizations for the same set of interview questions. Triangulation of multiple time was also used. Multiple time refers to the key informants were interviewed separately (not in a group setting) so that there will be no group influence while expressing their expert opinions and insights. Three groups of key informants were selected for the interviews. They were from government organizations, medical professional bodies and legal firms that engaged in the building or advising regarding the Ontario EHR program. Both qualitative and quantitative data were obtained during the interviews

This chapter is organized with Section 6.1 introducing the three groups of key informants (subject-matter experts) and the use of the qualitative triangulation research methodology. Section 6.2 describes the function of key informant interviews. Section 6.3 describes the methods and the instruments used to obtain data from a specially designed questionnaire. It also explains how data was reviewed and approved by key informants before acceptance into the research database. Section 6.4 describes the result of the key informant interviews with noted observations for further analysis in a later chapter.

Section 6.5 describes the results of the second part of the interview with semi-structured questions. Section 6.6 provides the preliminary findings towards some of the research sub-question. Section 6.7 cautions the scope and limitation before establishing the conclusions. Section 6.8 summarizes the chapter by identifying themes and issues raised by the key informants.

### **6.1.1 Three Groups of Informants**

Government organizations in this study were the payers of EHR. The responsibilities of payers included financial support, as well as creating the architecture and the implementation of the EHR initiatives. Within the government groups, there were informants from three key government organizations were interviewed. These included the federal crown corporation (Canada Health Infoway---CHI), the provincial health ministry (Ontario Ministry of Health), and the provincial level agency (eHealth Ontario) that implements the EHR system. CHI produces national architectures and frameworks of the EHR systems. Such architectures composed of an interoperable EHR framework and the standardization of EHR data flow and information across different sub-systems at a national interoperable level. Ontario Ministry of Health sets out Ontario's policy and strategy to be used by eHealth Ontario. eHealth Ontario under the strategic direction of Ontario Ministry of Health and takes the CHI's architecture and framework to perform further customization and detailed design for the specific needs of the province of Ontario.

Also, CHI provided part of the overall funding of the EHR program from the federal level to each province upon a satisfactory review of the provincial customization and requirement of the design. There is, however, an ample amount of freedom regarding provincial level customization. The provincial Ministry of Health has the overall responsibility for health care and health administration within the province. It ensures and guides eHealth Ontario in the production of the detailed design, implementation and adhere to quality assurance process of the provincial EHR system. From the discussion with government key informants group [Gov-GP], it was found that a closer working



relationship and communications among the three organizations could help a better implementation and delivery of the EHR program.

The author also observed that a multi-year government project needs strong political support. During the interviews, the direction of the EHR project was unclear pending the result of a political election. There was a concern that a change of government leaders could reprioritize the program execution. The second group of key informants was from medical professional groups [Pro-GP]. These key informants were from the federal level and provincial level medical professional bodies. These group of informants protects the interest of their members who are healthcare service providers and provides consultation over the implementation of EHR system. One of the informants was an executive who has created an operating health information system similar to the EHR system.

The third group of key informants was from legal firms [Leg-GP]. They were lawyers that have participated in the EHR project and were capable of providing insights regarding the EHR system. They discussed insights on the program and project capacity and the relationships among government organizations and stakeholders. Provider and patient information privacy and the security of sensitive information were also part of their interests in the EHR project.

## **6.2 Functions of Key Informant Interviews**

The objective of key informant interview is to understand the factors that influence the health service providers and ultimately the patients in their attitude towards privacy concerns in the EHR systems. Without the adoption of EHR from service providers and patients, the efficiency and efficacy of the EHR system will be significantly compromised. The discussion and insights in this chapter will seek to add further explanation to issues that were found with patients and service providers in the previous chapters. Payers provide funding, architecture, regulations and the implementation of the EHR system. Therefore,

their experiences and opinions regarding perceived benefits affect the providers and patients in operation, efficiency, and efficacy of EHR system.

Key informant interviewing is a critical technique in obtaining an expert point of view on issues and insights (Tremblay, 1957). Key informant interviews provide the following benefits in the context of examining privacy concerns with the implementation of an EHR system. They allow an in-depth semi-structured dialogue with subject matter experts who have insights and understand the assumptions used in the architecture, design and implementation of the EHR system. It provides a means to examine the intentions and limitations encountered in the implementation of the EHR systems and processes. Key informants can help understand the inter-relationship of issues and challenges identified in the EHR systems from the specification, to design and to implementation. The interviews also help identify challenges and expectations from the payer's perspective. The understandings of such aspects help uncover plausible reasons regarding the privacy concerns and countermeasures are taken by service providers and patients in this study.

Other benefits of key informant interviews are to understand the approach from the payers in determining the scope and framework of who are the users of the EHR system.

Further benefits include the ability of the researcher to clarifying the findings of the quantitative survey with patients and the qualitative results from the focus group discussion with providers. After compiling and analyzing the data from provider and patient groups, the initial insights gathered from key informants will be able to provide a probable or even plausible framework and reasons that help explain the behavior of service providers and patients when they engaged with the use of EHR system. Key informant interviews also help to triangulate the response of providers and patients. In summary, key informant interviews can improve the interpretation of the observations obtained from the providers and patients. Such understanding may explain factors related to the efficiency and efficacy of the use of the EHR system.

### **6.3 Methodology in Conducting the Key Informant Interview**

All the key informants interviewed were enrolled at arm's length to us with no prior relationship. Therefore, an objective discussion of the subject can be achieved. Key informants hold prominent positions in their respective organizations and are well qualified in their assessment and opinion to the EHR project. Upon agreeing to the interviews, key informants were sent a short survey form a list of semi-structured questions to be asked during the meetings. This provided time for the key informant to think about answers to the questions, issues at hand and the scope of the interview. These semi-structured interviews resulted in the discovery of information that would not have been revealed in a survey or focus group sessions.

Data quality is one of the challenges that is often found in qualitative research. This includes the issue of rigor, validity, and reliability of the data. Criticisms include concerns about self-reporting from the key informants and potential problems of bias. For this evaluation, various steps were taken to ensure that the data used was accurate and reliable. They included: (1) Ensuring an adequate number of interviews were conducted. (2) Developing clear guidelines on interview transcription and having the interviews transcribed by multiple persons. (3) Before data collection, procedures and guidelines were created that clearly outline the processes used for coding, analysis, and making conclusions from the data including describing the steps taken and decisions made in the audit trail. (4) Triangulating the data, both regarding using multiple data sources from different key informants and different organizations and even similar questions in the interview. (5) All interviews were taped and then transcribed into MS-Word. Key informants were given their transcripts to allow member checking of the transcribed data for accuracy on the contents and the context of the topics. Each key informant has their own schedule and freedom to correct and clarify their data from the interview. Only after receiving the key informant's validation of data, then such data would be officially accepted to the key informant research database.

To reduce data collection from group bias, and to facilitate data triangulation, different key informants and various organizations were used to provide multiple sources of data to the similar questions (Denzin, 2006). Nine key informants were enrolled in three different types of organizations. As stated earlier in this chapter, these organizations were involved either in the design, implementation as key stakeholders or as advisors to the EHR program. Government organizations provided perspective on funding, architecture and EHR system implementation. Professional medical bodies emphasize the view and the protection of the health service providers as key stakeholders. The legal firms provide expert opinions on legality, privacy, and security of the EHR project and the opinion on the protection of patient's rights to information privacy and security. Key informants in legal firms worked on the EHR project as consultants or advisors.

Another objective of the pre-questionnaire to key informants was to explore their opinion as to what Canada Health Infoway has publicized on the benefits of EHR systems. As the EHR program is still in progress, many sub-systems and their interoperability have not implemented. The data collected during the interview was based on the key informants' assessment of the status of implementation and their beliefs when the program is completed. It is believed that the key informants' assessments of the completed project will account for any critical inefficiencies and deficiencies as evidenced in the current project status at the time of interview.

The second part of the interview was a series of semi-structured questions with a selected framework of topics. Key informants were free to describe their assessments and perceptions and to add any sub-topics during the interview. These semi-structured questions include the following research objectives and specific topic areas. (a) To obtain key informant's comments and perceptions on information, privacy, and the security protection of EHR. (b) The impacts on the payers of EHR systems if patients withhold private health information. (c) The payers' expectations of patients regarding their cooperation (i.e., the full disclosure of all relevant health information when using the EHR system). (d) The technical and information assurance level of the protection of information privacy and security within the EHR system. (e) Through their experience in

the participation of EHR project, key informants are to assess current progress and challenges of the current implementation, which in their belief will reduce the efficiency and efficacy of the EHR system. Finally, (f) Generating recommendations of possible solutions to current issue or gaps - for example, interviews with EHR key informants help to define the gaps in their services and assist in identifying potential solutions or recommendations to resolve these issues.

#### **6.4 Results of Key Informant Interviews on pre-questionnaire**

Below shown the results of the key informants from government group, a legal group, medical and professional group as well as the legal group. The author emphasized that these group are experts so that even with a small interview group of three, their opinion are of professional level and thus the mean value of their answer is acceptable. An expert provides more accurate and carries a higher truthful value to that of participant enrolled from public, therefore, the statistical mean of their opinion is of value to the result and discussion.

##### **6.4.1 Results of EHR Benefit Statements from the Government Group**

Three government key informants were interviewed individually over three occasions. Therefore, their answers are independent of each other.

For the first part of the interview, the statements in the above table are the EHR benefits CHI suggests should occur with implementation. Therefore, it is reasonable to expect that the answers from the three government key informants should be a value of 4 (agree) or above. While the overall response to the benefits statement is a value of 4, four statements are below the value of 4.

For the statements on “security of personal health information” and “better protection of doctor-patient confidentiality,” both receive a 3.7 on the Likert scale

[PF46]: “Gov-GP” perceived that security protection of EHR is adequate but have a new challenge

Two of the three government participants “Gov-GP,” agree on the improvement. However, also indicated that there are new challenges (1) Increased access as it can now be accessed by many providers in the province. (2) Criminal hacking of the information could be possible. One of the participants indicated that patient-doctor confidentiality might not be adequately protected depending on the actual implementation.

The author suspected that the implementation of the protection mechanism in EHR is adequate in protecting both the security of health information and confidentially information between the doctor and patient. However, the new privacy risks are increased as information is now in electronic form.

For the statement “Reduced reliance on verbal exchanges of health information between provider and patient,” the key informants have rated it a value of 2.3, which is close to the “disagree” category on the Likert scale.

[PF47]: “Gov-GP” thinks that verbal exchanges of information are somehow reinforced but not reduce with EHR as per published statement.

Two of the three participants think that EHR will not reduce the reliance on the verbal exchange of information between patient and provider. It will, however, reinforce the verbal exchange.

In the opinion of the author, it is possible that the informants are concerned with the responsibilities of this statement that EHR may not be accurate or service providers still need to consult with another medical professional instead of merely rely on EHR. Before asking the above comments, key informants were reminded that these were the published benefits of the EHR program.

#### **6.4.2 Result Of the EHR Benefit Statements from the Medical Professional Association Group**

The medical professional group was composed of individuals from two medical professional associations from federal and provincial level. Also, the third key

informant came from an organization that has built an active electronic health information system that is similar to the EHR system. Since the government group leads the building of the EHR system, both the medical professional association group and the legal firm group are used to triangulate and validate the answers from the government group. Results from Table 6-1, show that the medical professional group rated a lower Likert value on nine statements; higher value on seven statements; and with the same value on two statements when compared to the government group. Overall, the medical professional association group has a similar Likert value of 4.0 for that of the government group. On some statements such as “There will be better patient privacy protection with EHR” and “Reduced reliance on anecdotal (based on personal experience or reported observations unverified by controlled experiments) exchanges of health information between provider and patient”, the medical professional association group is less than enthusiastic (-1.3 and -1.0) than that of the government group.

**[PF48]:** Professional group [Pro-GP] has a similar assessment with government group in the government published EHR benefits statement

Conversely, when considering the statement “Use of standardized health information will allow for faster review of health information,” the group averaged a rating to a close to the category of strongly agree (4.7 on Likert value) than that of the government group who only agree (4.0) on the statement

### **6.4.3 Result of the EHR Benefit Statements from the Legal Group**

The legal group has a more skeptical view on the government’s ability to deliver the claimed EHR benefits. The average score of all the benefits statements is a Likert scale of 3. When compared with the result from the government group, the key informants from legal group do not agree with the statement, “EHR helps the government to reduce rising health costs (such as duplication of lab tests and patient’s doctor hopping).” The Legal group rated an average of 1.0 -- - “strongly disagree,” and the government group rated an average of 4.3 --- “agree”). The legal group was also more critical on the “benefits of better

privacy protection of EHR” and “better protection of doctor-patient confidentiality. The difference in rating is -1.8 and -1.2 in Likert scale respectively when compare against the rating from the government group. The legal group was also critical on the benefit statements of “Accurate communications among providers” and “Reduction of duplicate test prescribed.” Both statements received a score of -1.7 value when compared to government group’s rating.

**[PF49]:** Legal group strongly disagrees that EHR helps the government to reduce rising health cost.

Both of the participants selected a strongly disagree with this statement. They cited the reasons are: (1) They do not believe that high health costs are due to health practice such as duplication of tests or patients doctor hopping which could reduce in EHR. The participant pointed out that high cost of healthcare is related to the cost of running hospitals, salary, and money put out for the drug. (2) The contribution of EHR benefits in saving the high cost of healthcare will be very insignificant and in a tiny portion within the portfolio of healthcare costs.

In general, out of eighteen benefit statements rated by the legal group, sixteen statements scored lower than the rating of the government group. One statement scored the same as the government group. Only one statement on the “reduce reliance on the verbal exchange between provider and patient,” the legal group is more optimistic and received a +1.2 in value. The 1.2 value comes from the government group rated a low (scale = 2.3), and the legal group rated a higher value (scale = 3.5, between neutral to agree category). The legal group has participated in the EHR to build a program with the provincial implantation organization. They have less confidence in the efficacy of the government in the delivery of the EHR program.



## **6.5 Results of Semi-Structured Questions from All Three Groups**

A set of semi-structured questions were asked from the key informants as in Table 6-2. Questions on the program size and resources available to the key informants were first asked with the purpose to establish the baseline information of the EHR program. It was then followed by questions directly related to the central theme of this research. They are the privacy and efficacy aspects of the EHR program. To explore some of the potential concerns from patients, key informants were asked probing questions to gain insights on how payer's actions might influence the opinions of the patients. The last part of the interview was used to gauge the overall satisfaction of the key informants and any lesson learned from their experience should they have the opportunity to execute the program again.

Baseline	(1) Are there any new benefits that you have identified but are not in the above list?
	(2) When you think about building EHR capacity on a provincial scale, are there any significant barriers/challenges that you are concerned about?
Privacy	(3) Please comment on your perception on whether there is the adequate patient-doctor protection of confidentiality in the EHR.
	(4) Please comment on your perception on whether there is adequate patient privacy protection in the EHR.
	(5) Please comment further on your perception on whether there is adequate information security protection of the EHR.
	(6) What are the perceived risks surrounding the sharing of private and sensitive health and personal information with health care providers and potentially having the information distributed across the health system?
Efficacy	(7) Are you aware of any gaps in the design of and the implementation of EHR?
	(8) Would you agree that your activities are now fully supported by the resources designated under the EHR strategy?
	(9) From a legal perspective, what are the challenges in EHR program, to the payer (government), provider (doctor) and the patient?
	(10) Please comment on the effectiveness and efficiency of the EHR programs, policies and services that have been implemented.
Probe for patient's concern	(11) What are your expectations of patients regarding patient cooperation (such as full disclosure of all relevant health information) in the EHR system?
	(12) What are the impacts to the payers of EHR systems if patients withhold the disclosure of private information?
	(13) Do you think that patients will withhold medical information from their health service providers due to concern about the inadequate protection of their private information?
Overall program	(14) What is your overall assessment and satisfaction of the EHR program?
	(15) If you were in charge of the EHR program again, what would you do differently?

Table 6-1: Interview questions

### **6.5.1 Baseline: Additional Benefits and Barrier to EHR**

#### **Additional Benefits of EHR**

Benefits published by Canada Health Infoway (CHI) are objectives that can be used to describe the efficacy of the EHR implementation regarding how closely the objectives are met. In assessing the payer's efficacy in the delivering of the program benefits, a baseline question ensures that significant benefits are included from the implementation of the program.

**[PF50]:** EHR could result in an extensive medical and knowledge database

When asked if there are any new additional benefits over the published benefits of the EHR programs, key informants from the government group [Gov-GP] indicated that:

- (1) Secondary use of EHR database could quickly provide vital and timely data for public health surveillance and management. This could help improve health interventions for not only one person at a time but broadly for health systems planning and analysis.
- (2) Remote access to information by the rural service provider.
- (3) The sizeable medical knowledge database is created
- (4) EHR repository of the medical database can be filtered with software

Professional KII group do not have any new benefits that they are immediately aware of.

The legal group [Leg-GP] indicated the benefits as:

- (1) To build an eventual development of Patient Health Records (PHR).
- (2) Agreed with Government group [Gov-GP], that public health management and data for research will be additional benefits.

### **Barriers or Challenges to the EHR Program**

A second baseline question was asked to the key informant in each interview; “When you think about building EHR capacity on a provincial scale, are there any major barriers or challenges that you are concerned about?” The purpose of this question was to identify any significant barriers or challenges so that it can be further explored in detail under the topics of privacy, efficacy or others later in the interview.

**[PF51]:** Deficiency of skillsets, integration and timely availability of implementation policy

The government group [Gov-GP] expressed that:

- (1) Efficiency in the design and consultation with a doctor about the EHR is significantly reduced because many doctors in their discussion were not Information Technology (IT) savvy and it was challenging to communicate concepts without defining and explaining the fundamentals of IT terms. It took time for the doctor participants to grasp the IT concepts especially when it comes to architecture and software data flow of information.
- (2) Another challenge was that EHR design and implementation has to integrate with all pre-EHR systems. There is the problem of connecting and integrating the many existing electronic medical systems into one EHR system via the government network. From a policy development perspective, the Ontario Government has the challenging task of aligning and connecting individual electronic health information systems that already existed and have been serving the function of EHR. Many such systems existed before the government EHR initiatives.
- (3) Another challenge is the integration with the existing Ontario privacy law, such as The Personal Health Information Protection Act (PHIPA), 2004. The function of PHIPA is to regulate the collection, use, and disclosure of personal health information in the healthcare sector. The purpose of the PHIPA law is to ensure proper implementation of the confidentiality and privacy of personal health information, yet permitting the efficacy of healthcare practice (MOH, 2004).

(4) Another challenge is to ensure the integrity and authorization of health information, such as how to connect data safely from laboratory systems to the rest of the EHR system. This required the preservation of the type, format, and the meaning of EHR data from the originating system to integrate flawlessly into the broader EHR system. From the implementation side, the key informants identified the feature of making EHR data available in a shared repository required a new approach to networked storage as opposed to the traditional method of individual healthcare service provider keeping the EHR data locally with the broader network connections. Many new policies and directions are needed before implementation. This shortage had reduced the available time initially allocated for design and implementation activities.

(5) Another barrier is the adoption rate of EHR are the resources available for EHR health communications, dialogs and education to patients and doctors. If the EHR stakeholder does not understand what EHR is, and what has been done to safeguard the critical and private information, it will be difficult to have the stakeholder adopt and use the EHR.

Key informants from the medical professional association were concerned about:

(1) There is little accountability of the government in implementation organization for the EHR program. (2) There were many implementation deadlines missed, and the priority of tasks had shifted and moved. (3) They also concern perhaps that service providers might fear the potential liability and extra uncompensated workload with the EHR system.

Key informants from the legal group [Leg-GP] pointed out that, in their opinion, the project management personnel were performing a project coordinating work instead of a project management functions

In response to point (2) above from the government group [Gov-GP], the author supplemented the point with an example of the pre-EHR system. Such example is the Electronic Child Health Network (eCHN, 2006) which was conceived in 1997 and was in operation in 2000 with five founding members including The Hospital for Sick Children and St. Joseph's Health Centre and so on.

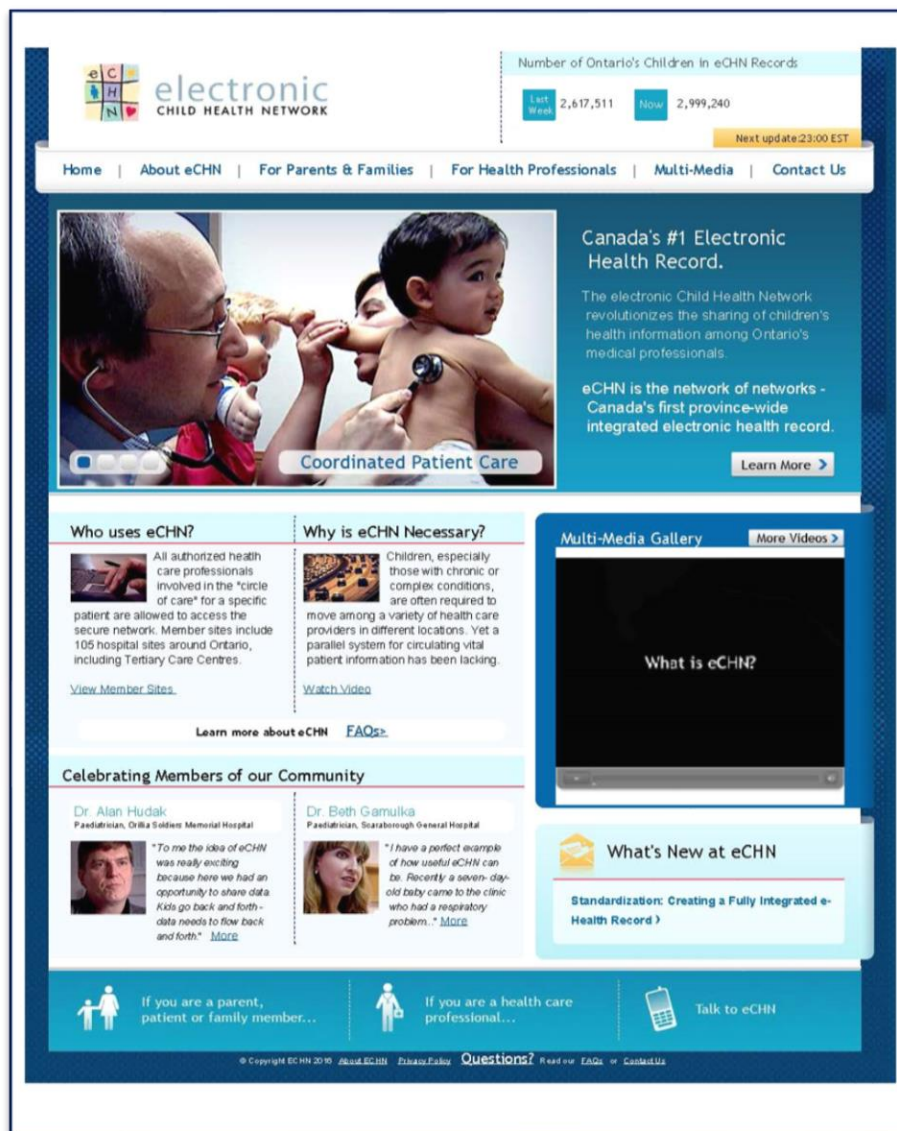


Figure 6-1: shows the online homepage of eCHN

## 6.5.2 Privacy: Adequacy of Protection of Patient Privacy

The second set of semi-structured questions to the key informants related directly to privacy. The first one was a direct question on the key informants' perception on whether there was the adequate patient-doctor protection of confidentiality in the EHR. The purpose of this question is to solicit key informants' assumptions when they design or implement the EHR system. It is important to recognize that the first time a patient made any judgment or attitude towards the EHR system would be a visit to his or her service provider who has adopted the EHR. Very often, this is their primary care physician. EHR information of the patient would then be generated based upon initial

diagnostics. Therefore, it is important to have patients feeling comfortable that their sensitive EHR is protected and their privacy is ensured.

### **Patient-Doctor Confidentiality**

In this question of whether there was the adequate patient-doctor protection of confidentiality in the EHR, the key information from the government key informant group explained the following points:

- (1) The EHR record is ordinarily accessible by many service providers who are authorized by the system, such as other doctors within the hospitals or other clinicians in the EHR system.
- (2) This might not be the understanding of the patients. Patients might reasonably think that their confidential EHR information could only be accessed within their circle of care (those service providers who are involved in treating and caring for their health in a particular instance of their sickness).
- (3) The EHR system does not segregate the service providers according to the circle of care but allows access to EHR information by anyone who is authorized to use the system. Authorization in many cases is based on their professional roles.
- (4) Therefore, in a hospital, a doctor or nurse is assigned with a role in the EHR system with specific role-based access privilege. Any doctor can access the EHR system even though the doctor is not part of the circle of care for a particular patient.

It was recognized by the key informants [Gov-GP] that to build trust in EHR system, it would require patients to feel comfortable in their interaction with service providers who act as their proxy in collecting the patients EHR data. To build this kind of trust, the EHR design and implementation team must provide adequate communication, increase the awareness of the benefits of EHR, and indicate what type of controls were in place to protect the patient-doctor confidentiality. However, this type of communication has not been widely established as most communications are to the service provider and communications to patients are mostly one-way communication in marketing literature or dissemble through websites.

The author noted that it is essential to accept a professional role for access to EHR in the system rather than “a care group” role as might be expected by the patients. A professional role allows the immediate takeover of the patient case, especially by another doctor who happened to be available or has particular expertise to see the patient’s EHR. This is especially so in an emergency department.

A broader question on the adequacy of protection of patient privacy in the EHR was asked to cover other issues related to access and use of EHR data. Such access included the public health management personnel and researchers in their potential analysis of EHR data.

**[PF52]:** Data are desensitized before available for research

Collectively, key informants had indicated that most of the EHR data would be aggregated and desensitize of patient’s personally identifiable information when being accessed for non-treatment purposes. However, they also pointed out that with approval from Research Ethics Board (REB), some personally identifiable information might be available to researchers.

**[PF53]:** Training for service providers is needed

Key informants recognized the need to provide education to service providers including administrators who have access to the EHR information.

**[PF54]:** EHR privacy protection cannot prevent leaks by humans

Even when the EHR system has built-in privacy and security protection, there was the concern that some service providers might discuss or leak patient information in a social setting such as in an elevator or at a social gathering. Key informants from the legal group [Leg-GP] have related that there have been cases where two service providers were chatting about a patient’s case in front of others such as other patient or hospital visitors. There needs to be more accountability and procedures to respect the EHR confidentiality protection process.

The author pointed out that the funding requirement of Canada Health Infoway (CHI) ensures the protection process includes an evaluation of Treat Risk



Analysis (TRA) and Privacy Impact Assessment (PIA) that had to be done before a sub-system can be implemented. Through a triangulation and cross interview with other key informants, we were informed that many of these processes were conducted at the last minute and some were on an ad-hoc basis. In this regard, the key informants from government group [Gov-GP], believed that there is sufficient privacy protection on a patient's EHR as TRA and PIA were performed and approved before implementation.

**[PF55]:** Lockbox not ready to implement yet

There was also a discussion about the use of "lockbox" function in the security system. The government key informant group explained that in EHR and many personal health record systems. A lockbox is an electronic software emulates the feature of a hardware lockbox and protecting specific information from unauthorized access. It is a security feature that allows specified users to access part or all of the patient private information to the particular request of the patient. Current EHR implementation has the lockbox feature, but it is not fully implemented to the extent that it can support a patient's request according to the government group [Gov-GP].

### **Perceived risks**

There was a discussion on the perceived risks surrounding the sharing of private and sensitive personal health information with health care providers and potentially having the information distributed across the health system. The key informants from the government group [Gov- GP], felt that:

(1) The risks are low for role-based access are implemented to access the EHR information. The current security protocol requires that a role be identified and the appropriate level of accessing privilege be based on the role assigned to the user who needs access. (2) Again, the concern about the intentional human infringement of the security protection was more of concern rather than a system role-based on a security breach.

In the author's perspective, there should be a requirement that government policies be available proactively rather than reacting to new technology, as may be the case in EHR implementation. This means that the policy needs to consider protecting vulnerabilities created by the use of new technology. For

example, privacy protection policy for the mobile network distribution of EHR information in the use of a wireless communication link or smart-phone data connections using a phone service provider's communication network. There should be some guideline or policies available as some of the data can easily be transmitted over a wireless network in the future.

### **6.5.3 Efficacy: Gaps in EHR Design and Implementation**

Key informants from the government group [Gov-GP], indicated that there were gaps in the benefits:

- (1) The area of long-term care, oral care, and eye care were just a few gaps that the EHR program had not included these practices.
- (2) There were changes of leadership in the EHR implementation organization resulting gaps in the stewardship, direction, priority, and allocation of resources on the EHR implementation.

The author has mentioned in the interview that eHealth Ontario had undergone five changes of leadership within nine years (three CEOs and two interim CEOs). It was noted that the subsequent changes in leadership have led to the mitigation of deficiency and narrowing of the many gaps. Further discussion on this issue which triangulates some important points around efficacy, will be discussed in Chapter Seven.

- (3) There were also gaps between strategy and implementation, between policies and implementation. According to the informants, when the implementation teams needed to address directions and have the design finalized, they found out that some of the policies had not been completed. This created a time compression situation in meeting the project deadlines.

- (4) Key informants agreed that, in principle, policy development on design or operations should first be developed before EHR project implementation. However, in practice, it was otherwise. For example, no specific policy at a provincial level available to address some issues related to privacy or interoperability when detail implementation issues come up. The

implementation team and the architects had to learn and understand the different requirements, capacities and the current standards related to the issue at hand before a policy could be defined. Such issues could have been identified if there was proper time available at the design stage and therefore policies could have been created before implementation.

**[PF56]:** Gaps in national standards and provincial implementation

Although there is national level design and architecture available from Canada Health Infoway, the provincial EHR team still has to refine and develop their specific design and policies before implementation.

**[PF57]:** Implementation under pressure to complete as fund justifications

Another group of key informants had expressed their opinion that the EHR program was not built from a functional perspective. It was built from delivery and “what is accomplished” perspective. Functional perspective takes a normal route of designing a system based on what end functions of the system should be provided. A delivery and “what is accomplished” is a system being built emphasizes the time of delivery and “what is accomplished” for the sake of justification of expenses or political accomplishment. Very often, such approaches compromised the quality of the function of the implementation with a decision to delivery first, pending correction and adjustment of features later. There is a need to demonstrate success to justify expenses, but the program is extensive and complicated even as of today. Proving success is difficult. This was one of the factors on the urgency to show or push out implementations to justify the expenses on the EHR program. Not having policy and strategy ready, was a significant gap in the implementation and created many performance issues.

Deficiency of Resources and Project Approach

According to government key informants [Gov-GP], there was an intention to conduct extensive EHR consultations with service providers before the EHR design. However, it was challenging to enumerate doctor’s participation. To many doctors, it was a matter of priority on this invitation for EHR consultation out of their busy and sometimes unpredictable work schedule. Another

challenge to the payers is in obtaining the right resources for the EHR program consultation. There was a shortage of Information Technology skillset in doctors to provide discussion on the technical aspects of EHR.

When asked about supports, key informants from the government group [Gov-GP] felt that they had the full support of government and the players involved to be able to address the issues of the EHR program. Key informants generally agree that there was a practice of aggressive implementation to the extent of implementing first and dealing with potential problems later. Even the key informants from the government group [Gov-GP], felt that the program is too complex and the skillset level of some of the developers and implementation team members was not adequate to deliver on the project. They also felt the pressure of a compressed schedule to implement.

Key informants confirmed the same concern of service providers as a custodian of EHR records. In addition to sending information to the EHR system, providers also have a copy of their records in addition to doctor's notes and comments that are only accessible by the creator of the record (the doctors or their organizations). There were concerns about EHR records being compromised or stolen or systems being hacked into on the service provider's network by criminals. These types of incidents may result in legal consequences for the service providers.

#### Perception of Effectiveness and Efficacy of the EHR Implementation

Key informants from the government group [Gov-GP], indicated that it was too early to evaluate the efficiency and effectiveness of the program, as many other sub-systems have not been implemented. This is in contrast to another key informants' perception. It was perceived by other key informant groups that the implementation was slow; decisions were ponderous and often overly cautious. When comparing to other Canadian provinces in implementing EHR program, the Ontario team took more time and was much slower. Even as the largest province with a 13.7 million (StatCan, 2015), Ontario EHR implementation was still considered slow when compared to how quickly other provinces implemented the EHR. The Office of Auditor General of Ontario's special report Oct 2009 (OAGO, 2009) indicated that \$1 billion had been invested in

EHR, Ontario was still near the back of the pack compared to most other provinces, and the value of this investment has not been realized.

According to some key informants' experiences, there have been cases where EHR implementation has been stopped because the EHR implementation team found out that they needed policies and strategies that were neither detected nor initiated. There was also the opinion that the government did not have a successful track- record of building large technology programs using complex and sensitive personal information in a national level architecture with provincial implementation. The effectiveness of the program has been challenged in many ways in areas of technology rather than from health services. Some key informants argued that regardless of the new electronic technology, doctors and patients have been using the technology for many years. EHR is a technology implemented in the existing health IT platforms.

#### **6.5.4 Probe for Patient Concern**

The third section of the key informant's interview involved some probing questions related to potential issues identified in our pilot survey with the patient.

A question on the payer's expectation of patients' cooperation was asked to explore any suggestion as to why some patients were not willing to provide complete information to the EHR system uncovered from the patient survey. The key informants from government group [Gov-GP], felt that it was a non-issue. Accordingly, the service providers are the main user, and therefore, the providers' participation counts towards the corporation. By law, as discussed in Chapter Four, the service provider is accountable for being the custodian of patient's health record and using these records to make medical decisions. The key informants from the government group [Gov-GP], believed that:

(1) The patient would provide the service provider with complete information. Although patients have a choice not to participate in the EHR system, they were not considered as the primary user of that information in EHR.

(2) The service providers are the primary users of EHR. It was expected that the patient would provide adequate and full disclosure to the service provider during the visit to the service provider who would then act as a proxy in recording the patient's EHR information into the system.

Key informants from the medical professional group [Pro-GP] have a different perspective on this question. They understand that:

(1) Government's implementation of EHR is using the service provider to obtain full disclosure of the patient's information. Therefore, by proxy, patients will be in the EHR system.

(2) [Pro-GP] believed that while the patient might disclose more information if they were sick but might not reveal as much private information during an annual checkup or for any non-serious sickness.

Key informants from the legal group [Leg-GP] pointed out that:

(1) Patient's cooperation could be much different when encountering an EHR shared database system vs. the traditional doctor non-shared health record database, and that some of the family physicians and specialists are still using. Patients would be more comfortable knowing that their personal health information remained only in the computing system in the doctor's office without being shared nor distributed to other computer networks. Otherwise, the records will be accessible by persons that are outside the circle of care.

(2) They also pointed out that patients have concerns about knowing who and why others access their health data. With these concerns, patients may wish to withhold the disclosure of their health and private information to the service providers unless it is necessary to care for their condition.

In Chapter Four, the resulted patient survey indicated a different level of disclosure is used in providing sensitive private information to patients. Some patients would only give some information instead of full disclosure even when they are sick.

### **Patient withholding information**

When asked about the impacts to EHR system if patients withheld private information to the EHR project, the key informants from the government group [Gov-GP], felt that there would be an insignificant number of patients who would do so. It was, therefore, not expected the impact of the EHR project.

Key informants from the medical professional association group [Pro-GP] indicated that there were cases where patients and service providers might withhold information from the EHR. They estimated that the cases of withholding of private (sensitive) information were around 10%. Their estimation included doctor unwilling to provide sensitive patient information such as a patient having a mental health condition or patient family issues. However, they believed that this withholding of information would have minimal impacts on the performance of EHR system.

Key informants from the legal group [Leg-GP] also indicated that there would be minimal impact on patients withholding information to the performance of EHR system except it would create inefficiencies and cost increases, such as patient's hopping from one service provider to another especially those doctors who do not use EHR system. [Leg-GP] expressed that if patients are withholding some information, service providers would have less information to make quality decisions. The provider might need to prescribe further, order repetitive tests to make a medical prognosis, thus reducing some of the potential efficiency gains of an EHR.

As part of the triangulation process, the author has asked similar questions later in the interview to confirm the validity of answers from key informants. When asked in a different question if patients would withhold private medical information from their service provider due to concern on the inadequate protection of their private information, key informants from the government [Gov-GP] expected that fewer than 1% of the patients would withhold information.

Key informants from the medical professional group [Pro-GP] reiterated the estimate of 10% of patients and doctors would withhold information. It is noted

that these are estimates from the key informant's expertise and experience in the EHR in Ontario. No document nor literature is supporting these estimates.

The key informants from the legal group [Leg-GP] indicated that some patients would be willing to give private information when they need treatment on their sickness but may wish to use a lockbox to make the same information unavailable to others once their sickness has been cured.

The author assessed that this might reflect the opinion that patient would balance their benefit before deciding how much personal information would be disclosed. This corroborates the perception that patient would be less willing to provide private information when they are only participating in annual checkups or a perceived non-serious illness.

#### **6.5.5 Overall Project Impact**

The last part of the semi-structured interview was to ask the key informants their perception of the overall EHR program.

When asked about the overall satisfaction of the EHR project, key informants from government group [Gov-GP] pointed out that the program was far from complete. It was too early for them to express an opinion on the overall EHR program. The author noticed that there was the appearance of caution in answering this question as it could reflect on their performance in the EHR program.

The key informants from the medical professional group [Pro-GP] expressed some reserved satisfaction. They pointed out that the EHR program still needed much work to complete and the full benefits could only be recognized with high participation and majority of the EHR system being rolled out. However, what was implemented so far could have been done much better.

In expressing their satisfaction with the EHR project, the key informants from the legal group [Leg-GP] pointed out that the EHR program is a public government project with design and implementation responsibilities. In their opinion, the characteristics of the EHR project carried all the government style



of big spending, large and complex nature with multiple jurisdictions and political intents. From this perspective, they were in a neutral position as to the overall impression of the project. They were neither very satisfied nor very dissatisfied given the premises that it is a government public project.

The last question in the interviews was to imagine if the key informants have an opportunity to do the EHR program all over again, what would they do differently. Key informants from the government group [Gov-GP] said that they would develop more policies before implementation. They would also have more structure and resources in place.

The key informants from the medical professional group [Pro-GP] would like to ensure the IT system be addressed with a precise definition of issues and what needs to be resolved. In other words, more simulation and study before design and implementation. The strength of the EHR system on design and standard was good, but some policies in privacy and security needed to be defined and established. They would also make additional efforts to involve patients with the EHR program.

The key informants from the legal group [Leg-GP] suggested that they would use a bottom-up approach instead of the current top-down approach to design and implement the EHR program. They would adapt and integrate local standalone electronic health information system (a pre-EHR system that does the same functions) into the design.

## **6.6 Preliminary Findings on Payers' Response Towards the Research Questions**

Iteratively, the following preliminary findings [PF] are related to the items listed below within each research sub-question. These PFs will be triangulated and review and analyzed in Chapter 7.

The research sub-questions identified in Section 2.7.1 are

*Q. What are the challenges and concerns of payers in their implementation of EHRs?*

Barriers or Challenges to the EHR Program

[PF46]: “Gov-Gp” perceived that security protection of EHR is adequate but have a new challenge

[PF48]: Professional group [Pro-GP] has a similar assessment with government group in the government published EHR benefits statement,

[PF49]: Legal group strongly disagrees that EHR helps the government to reduce rising health cost.

[PF51]: Deficiency of skillsets, integration and timely availability of implementation policy

[PF53]: Training for service providers is needed

[PF54]: EHR privacy protection cannot prevent leaks by humans

[PF55]: Lockbox is not ready to implement yet

[PF56]: Gaps in national standards and provincial implementation

[PF57]: Implementation under pressure to complete as fund justifications

[PF47]: “Gov-GP” thinks that verbal exchanges of information are somehow reinforced but not reduce with EHR as per the published statement

**6.6.1 Other Observed Preliminary Findings**

[PF50]: EHR could result in an extensive medical and knowledge database

[PF52]: Data are desensitized before available for research

## **6.7 Scope and Limitations of the Evaluation**

Regarding scope and limitations of the evaluation, this part of the data collection mainly focuses on payers of the EHR system and their perceptions regarding the implementation of the EHR system at a program and functional level. There is no attempt to explore individual sub-systems of EHR system. Examples of such sub-system are “imaging diagnostics” and “lab repository” systems.

A comprehensive evaluation of how the payers designed and implemented the EHR is out of the scope of this research. Instead, the operational impact on EHR and perceptions from the provider and patient groups were studied. Such impacts were a direct result of the payer’s implementation and policies surrounding the EHR. Also, the key informant interviews were conducted with some key individuals who have the depth of knowledge about the contents of the design, benefits, and policy for EHR implementation, while other key informants were more knowledgeable on the impacts on service providers and patients in the EHR system. An essential limitation of this evaluation work is the lack of reporting available on the performance assessment system for the EHR program. There is limited information from the previous implementation reviews and audits published by the Ontario Auditor General. As a result, this exploratory study, by necessity, takes on the characteristics of a point-in-time examination of implementation, while establishing the possibility of follow-up work in support of the EHR design objectives verification. Key informants were required to provide their retrospective assessments of the performance.

Another limitation is very few valid assessment tools in the area of electronic health informatics for the EHR interview and evaluation have been developed. There is a paper titled “Formative Evaluation of the Integrated Strategy on Healthy Living and Chronic Diseases” from Public Health Agency of Canada PHAC (2009). This framework adopts those mentioned above “Formative Evaluation” paper using a similar methodology in assessing the implementation of EHR in Ontario. Hence, we have developed an interview guide specifically for this exploratory interview and evaluation of EHR implementation. While

there may be some limitations in this evaluation, mechanisms will be in place to address these limitations where possible.

## **6.8 Chapter Summary**

This chapter is important in obtaining the perspective from key informants from the government, legal and medical association (subject matter expert) on their opinions and assumptions about the design and implementation of the EHR program. It provided insights that could explain the concerns of service providers and patients in the area of privacy and security. The assumptions from government key informants that patients would be fully compliant and there would be no impact if patients withheld their private information to the EHR system contradicted the results of our patient survey. The key informants from medical professional association group and legal group [Leg-GP] provided unique and different insights of the EHR program from their different roles to the government group. In addition to the many new insights, these two groups also provided triangulation in the source (i.e., different from the government group). All key informant interviews were also triangulated in space such that each key informant was interviewed alone in a different time and space (generally in his/her office) from each other. Therefore, their opinions and insights were not affected by other key informants. Chapter Seven will be a discussion of overall issues with analysis and the results assertion of thesis found in this research.

## **Chapter 7 Research Findings**

### **7.1 Introduction**

This chapter examines and synthesizes the results presented in the earlier chapters using the theoretical model and frameworks for the patients, providers, and payers. The discussion and synthesis start with the primary research model that uses the four dimensions in CFIP to ground the foundational question if patients have genuine concerns regarding their information privacy in EHR. Upon such foundation, the primary research question and sub-questions are built. The ranking of the order of privacy concern in this study is presented. It is also compared with a previous research study that uses the four dimensions in CFIP. The discussion continues with the evidence gathered using the theoretical frameworks from Section 3.7 in the research methodology chapter. Afterward, the preliminary findings identified in Chapter Four to Six will be triangulated and synthesized into “Type 3, 2 and 1 Findings” in according to the triangulation design set out in Section 3.9. Due to the process of triangulation with survey questions and focus group discussion asking the same question differently, some part of the discussion will be reiterated in different topics. Five themes emerge from the triangulated findings.

## 7.2 Quantitative Framework for Patients: Ranking of Privacy Concerns

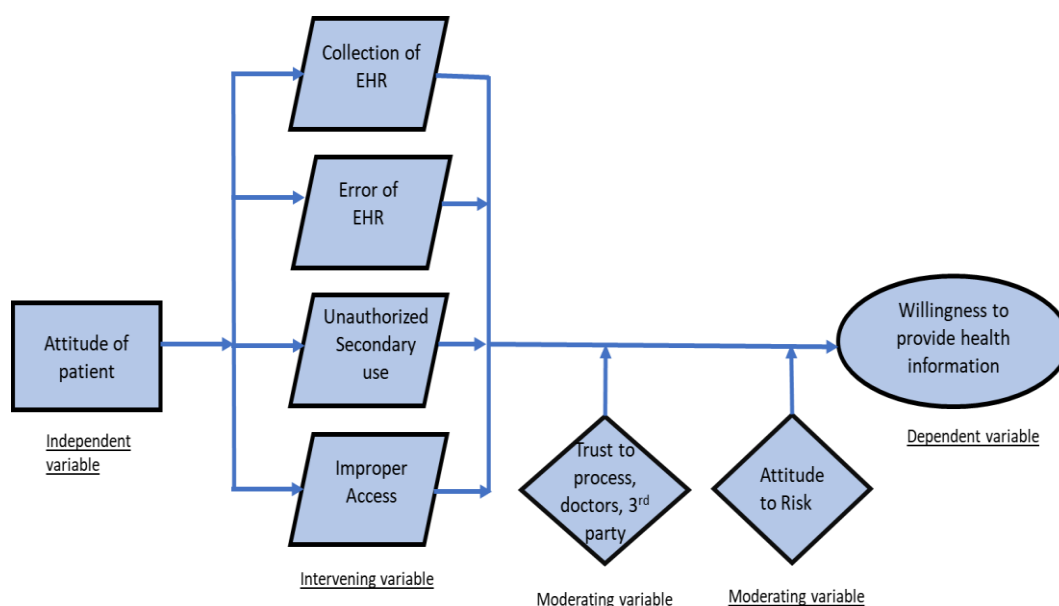


Figure 7-1: Quantitative survey framework for patients (from Figure 3-2)

Patients' Privacy Concern in EHR is Genuine. Examining how substantial, patients are concern about their information privacy in EHR, is a cornerstone upon which the research questions are constructed in this study. Patients have genuine concerns about their private and sensitive information as evidenced by the result of the quantitative and qualitative scenario survey in the research frameworks in Section 3.7.1. Three of the four dimensions of the CFIP model received high mean values of 4.75, 4.72, and 4.52 in the dimensions of "Unauthorized Secondary Use"; "Improper Access"; and "Error." These levels of concern are substantial and worrisome for patients to the extent to exercise various countermeasures to reduce the risk impacts of any privacy breach to their private information in EHR. The behavior of using countermeasure coupled with high mean-values in the CFIP dimensions as well as strong responses to the qualitative scenario questions in the same survey form confirmation and foundation to examine the research question in EHR.

One of the research sub-questions is to study the triangulation of the providers' attitude against the patients' attitude towards privacy concerns. The results

yielded a substantial similarity that provider echoed genuine privacy concerns in EHR. Coincidentally, providers exercised countermeasure for the similar risk mitigation as the patients. This appears to suggest a pattern of risk and privacy concern to those (patients and providers) who have provided their input data to the EHR system.

Regarding ranking the order of privacy concerns in the CFIP dimensions, the results of this study shown in the above paragraph correlated well with both Smith *et al.* (1996) and (2009) findings in CFIP. Smith's paper cited the "highest levels of concern were associated with Improper Access and Unauthorized Secondary Uses. (Smith *et al.*, 1996, p.188) whereas, Angst and Agarwal ranked

In Angst and Agarwal (2009. p. 369) study, the dimensions of Improper Access and Unauthorized Secondary Use are the first and third ranking of privacy concern. In this study, the exception to a high mean value is in the Too Much Collection dimension which shows a bimodal (similar number of patients are either disagree or agree) result.

Despite some patients expressing no concern of "Too Much Collection" providers indicated otherwise. Although the survey shows, patients' attitude is more towards disagreeing (mean value of 2.76) that there is "Too Much Collection" in focus group one pharmacist and nurses revealed their experience and claimed that it is common to encounter patients withholding information.

A plausible explanation of this evidences is that as there are about the same number of patients that are above the 2.74 mean value (in the agree and strongly agree) category that they are concerns. It is likely that focus group one that sees those patients withholding information are patients that have expressed an attitude of agree or strongly agree that there is Too Much Collection of their information.

Overall, except for the "Too Much Collection" dimension, the quantitative data from this research study shows a good correlation with the Smith *et al.* (1996) and the Angst and Agrawal (2009) studies.

### **7.2.1 Highest Privacy Concern is the Unauthorized Secondary Use**

The highest privacy concern described by patients is the Unauthorized Secondary Use of their EHR information. Four variables within this dimension are used. To achieve inter-question validity, NOU was used as a triangulation of time to the NOP variable. It has validated the attitudes of patients towards the “use of EHR data for no other purpose. Patients are consistent in answering both questions.

For the patients, they seldom know who sees their EHR information. This unknown creates uncertainty, and patients’ worry that should their private information is used by people outside the circle-of-care. “Unauthorized Secondary use” connotes the use of EHR information other than the primary purpose of treating the patient’s health without patient’s consent. Patients concerns are justified as they learned of cases of unauthorized secondary use of EHR as described in the literature review chapter. As discussed in Chapter Three, regarding the concepts of privacy, and author’s extension of such concept to EHR, patients have the right, [Flaherty (1991) on the Utility of Constitutional Rights to Privacy and Data Protection] to keep their private information secret. Patients’ expectation of such enforcement now rests on the providers who act as custodians of their health information and the payers who designed and implemented the privacy protection in EHR. When protection of patient’s private information is breached, patients could no longer enjoy the entitlement to be let alone as an unauthorized person would have a copy of their private information (Warren & Brandeis, 1890; Thomson, 1975, Sparkes, 1981; Harman, *et al.*, 2012). This perception is also reflected in the responses to the scenario questions (SSWC) in Section 4.9.2. Approximately 77% of all respondents were willing to take action to restrict the sharing of their private information with third parties. Such patient’s concern is in contrast to the viewpoint of payers who believe that patients will cooperate with their service providers and consider privacy is not a primary concern to patients when they are seeking medical treatment.

When triangulating the patient's concern of the unauthorized secondary use of EHR with providers and payers, this study finds that providers have similar



privacy concerns as patients. Service providers' concern of the unauthorized use of their portion of medical notes or information they inputted into the EHR, is being used by users outside of the circle-of-care for other purposes, which could be detrimental to their professional practice and career. Providers are also concerned that regulatory organizations review their inputted EHR information for reasons without their awareness. Other concerns include patient's litigation on their practices and unrelated peers viewing of their the EHR. In the case of distribution of EHR data for other purposes, payer maintains that data in EHR is sensitized using a similar process in protecting the identity of the owner of the information. This protection mechanism is seldom communicated to the patients and providers comprehensively especially in a non-technical context. It is inevitable that patients and service providers are concerned that they could be victims of unauthorized access and unauthorized secondary use of their private and sensitive data in the EHR. For them, the natural and most comfortable protection mechanism is the use of countermeasures to minimize the risk impact as they have no other control readily available to reduce the risk.

### **7.2.2 Second Privacy Concern: Improper Access**

Traditionally, patients depended on service providers to maintain their paper records with proper storage and theft protection. With EHR in electronic form and accessible over a computer network, patients expressed expectations that service providers should continue to implement new electronic means of protection to prevent unauthorized access to their private medical information. Eight in ten patients expect service providers to take necessary steps to prevent unauthorized access to their private and sensitive medical information. Such expectation includes the security compliance in the computers in providers' office (where a copy of the EHR data of their patients is stored) and the ethics of not discussing a patient's private information in public or unprotected areas around other patients. Patients are also in strong agreement that service providers should protect computer databases that contain their personal health information regardless of cost (DPU) and devote the necessary time and effort (EUA) to protect against unauthorized access. The purpose of the DPU

question is to reconfirm an earlier question if the patient would alter their expectation if service providers have to protect patients' private information even at all costs.

In the focus group discussions, service providers did not have significant concerns with the cost of protecting the system other than a smaller office practiced by a single service provider. There might not be comprehensive policies and procedures in place to protect against unauthorized access. Payers' opinions of the probability of unauthorized access were low as role-based access privileges were designed into the system. Key informants from the government group indicated the use of multiple factors of user authentication before allowing access to EHR system. There are standard procedures and secure encryption algorithms that can be used to protect patient records. However, payers have not sufficiently communicated this protection to patients.

### **7.2.3 Third Privacy Concern: Error of information**

In medical laboratories, patient name and date of birth are verified to confirm their identity before administering a test. Patients trust their service providers in not making errors in their data. They expect service providers to input the data correctly and that if an error is detected, it will be corrected promptly so as not to compromise the due care of their privacy. Such expectation is evidenced by the ARC variables with 86% of patients agree or strongly agree that all personal health information in computer databases in the service provider should be double-checked for accuracy, regardless of costs.

Providers taking preventative action is a necessary step to ensure accuracy as it is high on patients' expectations and building trust relationship. Patients rated the "correction of error" as the highest priority among the four variables above. The interpretation is that patients believe that service providers are unlikely to make an error on their records in EHR as the consequences of using incorrect or inaccurate data in EHR could be of dire consequences. Witnessing many provider's processes of the practice of double-checking before administering any medicine or procedure to them, patients trust their service provider's

process and professionalism to avoid mistakes. Patients believe that service providers are capable of managing data errors. They believe that providers will undertake the professional due-diligence of checking data for correctness in the EHR database and especially using such data when treating patients.

While Focus Group One with nurses and pharmacists (providers) confirms this practice of double checking for correctness, the group also indicated that there is not much time to investigate if an error was found. The incorrect data would merely be corrected and the work move-on. It appears that time is of the essence when treating patients and that mistakes will just be corrected. Given this practice, it is likely that systematic errors (that error will repeat itself), will not be corrected. This research study does not attempt to investigate the workload, the pressure and fatigue of service providers relate to the input and use of EHR. In the design of EHR, Payers have a technical check for error using traditional database technique. It is likely that patients expect more procedure on privacy protection from human hackers and unauthorized users rather than merely relying on what the EHR system has designed. Patients may not be aware of the provider's practice of not investigating simple or system errors and the payers offering of error correction relying on a technical solution of checking.

#### **7.2.4 Fourth Privacy Concern: Too much collection**

The result of privacy concerns on Too Much Collection follows a bimodal pattern with extreme polarization between “strongly disagree” and “strongly agree” categories. Two clusters of patients emerged: one group of patients that agreed “Too Much Information is Collected” whereas the other group disagreed. For those who responded “disagree” or “strongly disagree,” there are plausible explanations. One is the belief that questions asked by doctors are valid and important. Such questions, even those very private and sensitive in nature, are tools to diagnosis illness and therefore, necessary to come up with an appropriate treatment plan. For those who agree or strongly agree that there is too much collection, the plausible explanation could be that there is already

effective legislation controlling the collection of sensitive information. Two pieces of legislation could influence the attitude of the patients in their agreeing that there is “too much collection of information.” They are: (1) the Canadian Personal Information Protection and Electronic Document Act (PIPEDA) (OPC 2000) and (2) the Personal Health Information Protection Act (Cavoukian, 2004). Both pieces of legislation have limited organizations only to collect necessary and relevant private information. Patients believe providers can keep their data safe. One could relate that patients are setting their expectation as there are real concerns about losing their benefits. Such concern is reinforced with the media’s frequently published of security breaches of electronic data and the resulted loss of privacy.

Patients rely on doctors and care providers in treating and diagnosing their illness. Almost 30% of respondents are neutral in their opinion on this question as this could be an education issue with the patient not knowing how EHR protects their private and sensitive data.

Another finding from the patient survey suggests that as illness worsens, patients would be willing to give service providers more of their private information. The scenario questions in the survey showed that patients are interested in setting up privacy profiles in the EHR system to specify who can access their private information. A simple requirement can be fulfilled with Lockbox software inside the EHR system.

To the patients, the purpose of providing information to EHR is to help to treat their illness. Too much collection of their private and sensitive information in the EHR system invokes their concerns about the risk of privacy breach such as unauthorized secondary use. This study shows that patients are thoughtful and they are balancing the needs of treatment and the need for their privacy protection. Doctors do not see any issue in collecting information from patients as most cooperate and respect the professionalism of service providers. In contrast to the patients’ concern, it would be to the interest of payers to collect as much and as detail information in EHR to build an extensive medical database. With these details, the management of public health, the evaluation of

the efficacy of performance and perhaps the costs of healthcare could be better understood and controlled.

**7.3 New Intervening Variable Emerged in Patient Qualitative Scenario Survey**

As the results of the original four intervening variables in the qualitative scenario survey are enumerated, a pattern of intense actions to counter the effects of losing the quality of healthcare and benefits appears. This pattern of counteractions can form a new intervening variable for future study, which the author refers to as “countermeasure.”

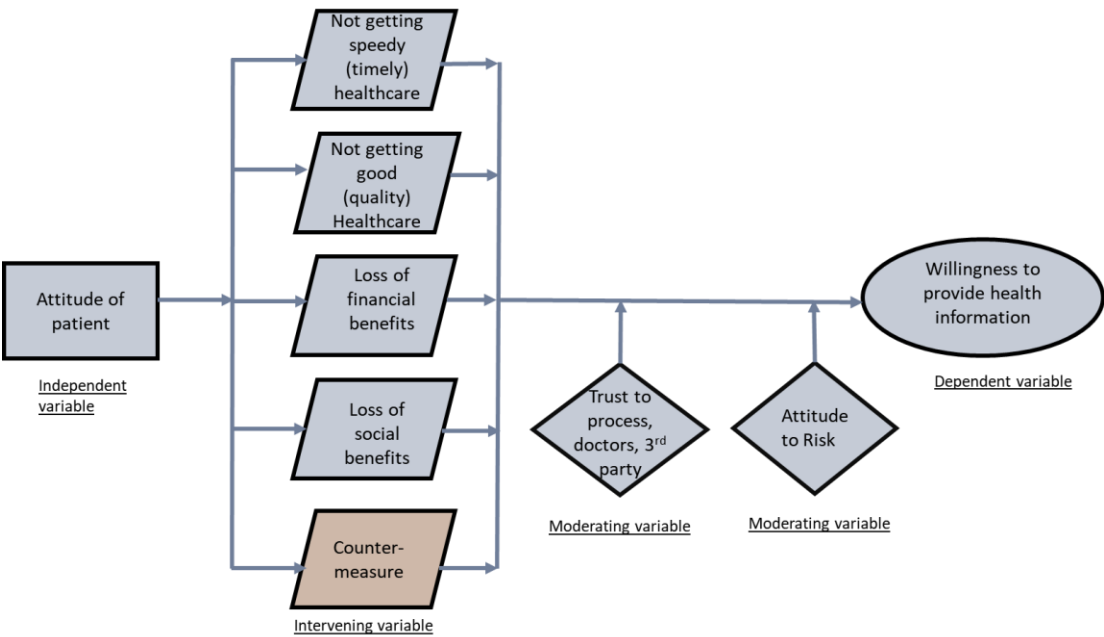


Figure 7-2: New Intervening Variable emerged in Qualitative Survey Framework for Patient on Scenario Questions

Patients use countermeasure as an action to mitigate the risk, vulnerability and dampen the impact of privacy exposure. Preliminary Findings from Chapter Four, [PF 6, PF7, and PF10] show patients will take actions and express a desire to control the privacy exposure of their private and sensitive information in EHR. The concept of countermeasure is explained in Section 2.8, however, to

reiterate, it is patients' action whereby they directly mitigate the perceived risk from privacy exposure. The intervening variable found in this research confirms the concerns of the vulnerability issues of digital information stated in the literature from Ravi (2008). The countermeasure surveyed in this study using the above framework (Figure 7.2) shows the how Ontario patients may take evasive and countermeasure actions to protect their privacy from the perceived threat of privacy breaches. Such countermeasures resonate with similar findings from California HealthCare Foundation (1999) as discussed in Section 2.9. Furthermore, the action of countermeasure from patients results in a reduction in the dependent variable of "Willingness to provide information" in the framework.

#### 7.4 Providers' Framework: Ability to Provide Quality Care in EHR

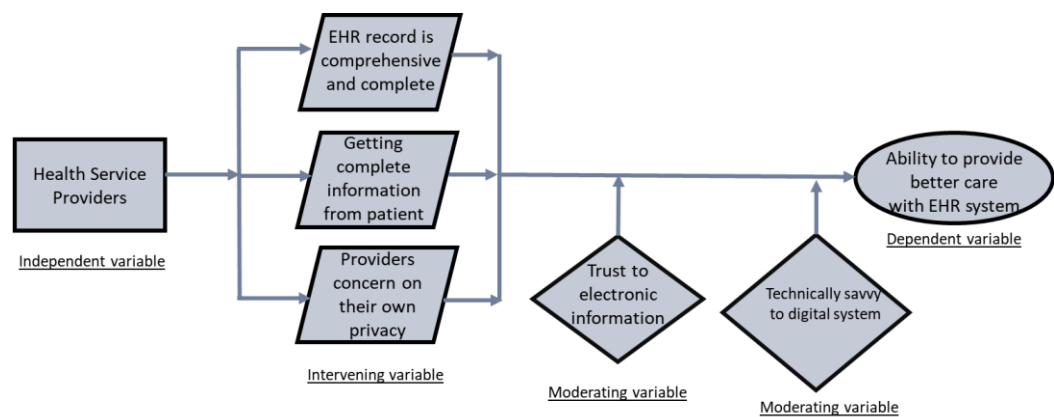


Figure 7-3: Providers Framework: Focus group discussion framework (from Figure 3-4)

The above providers' framework (from Section 3.9.2) is used to study the ability of providers to deliver better health care using EHR systems. This study found that with the EHR system, providers' ability to provide better care improved efficiency, especially with a holistic and comprehensive patient medical history available at the same time. However, the ability to provide better care is also reduced for the following reasons: (1) Incomplete EHR systems as modules are not fully implemented. (2) Interoperability of EHR

transferred between hospitals are still limited due to incompatible systems. (3) Incomplete or even incorrect information when patient withholds their private and sensitive medical information with the various types of countermeasures. Moreover, finally, (4) Providers secretly coded their private and sensitive information to avoid litigation and to protect patients privacy on unconfirmed illness, therefore, diminishing the system objective of open and sharing of EHR information to other providers.

The duality functions of providers place them in unique roles. On the one hand, as a user of EHR, they have to show confidence and calm the fear of privacy concern from patients. On the other hand, providers are also the owner of their data that they input to the system. They endure similar privacy concerns and also exercise countermeasures in EHR systems.

## 7.5 Payers' Framework: Realization of Benefits

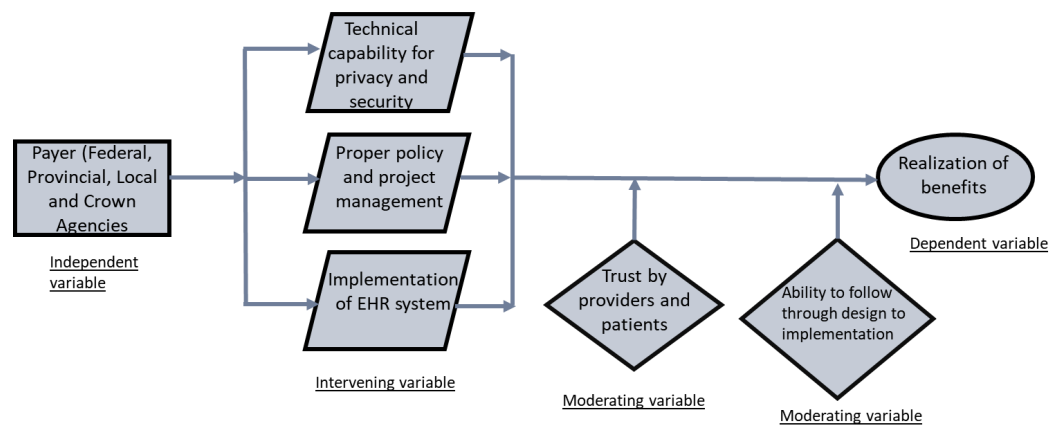


Figure 7-4: Payer's Framework: Key informant interview framework for payers (from Figure 3-5).

The objective of the payers' framework is to understand the alignment of the design and management of EHR towards the realization of the published EHR benefits. From the analysis of key informant interviews, the findings are: (1) Payers neither undertake sufficient consideration nor the attention of the privacy needs of patients. As a result, a technical solution to protect the privacy and security of data in the EHR system was built that does not meet the needs of the patients. (2) The unstable organization structure with a high turnover of Chief

Executive Officers in eHealth Ontario and the hiring of many temporary consultants did not provide stable corporate governance and design environment for EHR system. Finally, (3) the compressed time and ineffective project management caused delays and incomplete implementation of the EHR system. The above findings have created misalignment and issues towards the realization of the published benefits.

## **7.6 Critical realist Interpretation**

Without the opportunity to interact or find out the details of EHR, patients have not gained a good understanding of how the EHR systems protect their private and sensitive data. Critical realists believe that there are unobservable events that were caused by observable ones; hence, the social world can be understood only if people understand the structures that generate such unobservable events (Larsen *et al.*, 2015). As hypothesized in Section 3.3, patients' attitudes towards the privacy concerns in EHR, via the observable events from social world and interaction with the provider, could be a result of the payers and providers actions and designs. Such action and designs are related to the structure of EHR systems (including choices made for the EHR system) These actions are not readily observable by patients. Payers did not conduct consultation, and communications with patients, resulting in their lack of awareness of the privacy concerns of patients. With payers' belief that patients are not the users of EHR, there is little time allocated to perform needs assessment with them. Providers have their own issues in learning to input and using the EHR; it would not be their priority to observe and feedback to the payers if there are any privacy concerns from the patients. Besides, providers primary concern with treating the patient's illness and also, they have their own privacy concern in EHR that they have to mitigate. Within this EHR setting from payers and providers, patients source of observable events related to privacy concerns would be from media and discussion with other patients. Another source of observable events for patients will be their experience



resulting from breaches of their private data such as insurance company reducing their benefits or third party calling them to market products related to their illness.

Should the payers have made an effort in communicating and training the patients and providers on their concern, it would be an opportunity to close the gap for patients and providers to improve their understanding on privacy protection in EHR which could ultimately reduce their concerns and reduce the incidents of countermeasure. Payers are the principal actors to increase EHR transparency with observable events for patients and providers which then could address privacy concerns in EHR. Such actions will increase the efficacy and increase the benefits of EHR.

## **7.7 Gender and Age Group**

Is patient's age group or career stage a factor influencing the level of privacy concerns? This study shows no significant difference in gender preference between males and females in their rating of CFIP dimensions. In the area of privacy in EHR, the results obtained are in contrast to published research studies. Such studies are from Frost *et al.* (2014) and Walrave *et al.* (2012,) which suggested that females are less willing to share private information. Age group in this study is segregated using a convenience method with the division of the age group into career stages based on a liberal age denomination and as a unit of analysis to interpret the results in a meaningful way. An examination of the evidence from the survey showed that in the dimensions on the concerns of "Errors in data"; "Improper access to data" and "Unauthorized secondary use of data"; there is a high degree of agreement across the career stage groupings. Only on the "too much collection" dimensions where more females than males disagree that there is too much data collection, which also contradicts published research suggesting that female are less willing to share private information, suggesting they agree that there is too much data collection.

## **7.8 Type 3, 2 and 1 Findings after [PF] Triangulation**

A triangulation design, specified in Section 3.9, Figure 3.7, is used to assimilate and synergize the findings among the 3Ps. Below are the Preliminary Findings (PFs) found with each of the 3Ps based on the research data and evidence.

There are twelve PFs established in the patient's survey while thirty-three PFs are found in providers focus group interviews. Payer's key informant interview yields twelve PFs. The number of PFs found in provider's group is significantly higher than the other groups because of two reasons. Firstly, there are two focus group interviews were conducted versus only one survey questionnaires in patient's group and eight similar semi-structured key informant interviews weres done, one for each payer. More importantly, for the second reason, providers have to work with the other 2Ps (dual focus) in the EHR system. One focus on the payer design of EHR and the other focus is to provide healthcare treatments to patients. Therefore, providers have more opinions of the EHR system, and thus, more preliminary findings can be found. This, in contrast, that patient is the single focus by only seeing the providers while payers are also a single focus working with providers. These 2Ps only have to interface with one single group (the providers). To increase depth and effectiveness in understanding the table below on preliminary findings are grouped by each of the 3Ps and then further classified under each research sub-question and theme. Five themes emerged from the findings. They are Privacy, Countermeasures, Efficacy, Benefits, and Training.

	Research Sub-Questions / New Findings in themes	Preliminary Findings
<b>Ch. 4 Patients</b>	Q.1	PF1: There are privacy concerns on all four CFIP dimensions.
	Q.2	PF2: Most patients will give out private information if sickness worsens
	Q.2:	PF8: Getting treatment is more important than social embarrassment
	Q.2	PF9: Even with the financial loss, 50% of the patients will disclose private information to get treatment.
	Q.2:	PF11: When in an emergency 50% of the patients surveyed will disclose private information to the provider.
	Q.3	PF3: Only 50% of Patients believe that provider can keep EHR secure.
	Q.4	PF4: There is no difference in gender on three of the four CFIP dimensions except the “too much collection” dimension. Decrease trend of neutral. Still concern of privacy
	Q.5	PF5: There is no difference in the career stages (age groups) on three of the four CFIP dimensions except the “too much collection” dimension.
	Q.6	PF6: 95% of patients would like to have some control of their EHR data
	Q.6	PF12: 93% or patients like to have control over their private data in EHR. Training and Education are needed.
	Countermeasure:	PF7: Most patients (93%) will take action towards providers if their privacy is violated.
	Countermeasure	PF10: In the variable SDWC (Disclosure with Countermeasure), which 92.3% of patients will actively initiate actions (countermeasure) with the service provider.

Table 7-1: Preliminary Findings from patient’s survey and scenario questions

	Research Sub-Questions / New Findings in themes	Preliminary Findings
<b>Ch. 5 Providers</b>	Q. 7	PF17: Providers felt that time-consuming in inputting the EHR
	Q. 7	PF19: Verbal exchange of information can be overheard.
	Q. 7	PF20: No full patient's privacy
	Q. 7	PF25: Patient withhold information or walk away
	Q. 7	PF31: EHR solves some but also creates new problems
	Q. 7	PF34: Information hard to find, perhaps lack of training
	Q. 8	PF21: Patients can have access to their part of EHR
	Q. 8	PF22: There is an opportunity for unauthorized access to EHR information
	Q. 8	PF28: Concerns about the secondary use of information against providers
	Q. 8	PF29: Provider concerns about the increase in lawsuit
	Q. 8	PF40: EHR may expose doctors to litigation
	Q. 8	PF41: Concerns about using EHR to evaluate productivity
	Efficacy	PF18: Critical information include: Medication history, allergy warning, treatment history and drugs taken history in addition to the usual demographic information of the patient
	Efficacy	PF23: Patient using lockbox may compromise the quality of treatment
	Efficacy (Training)	PF35: Doctors need medical history, medication history, treatment history
	Efficacy (Design)	PF44: Information Security protection is responsible for Government, Cybercrime needs legislation
	Risk	PF13: EHR has benefits but also has risks such as accuracy of information
	Efficacy	PF14: EHR will increase efficiency and makes provider's work easier
	Benefit and Efficacy	PF15: Reduce medical errors and improve quality of checking
	Negative Efficacy	PF16: Implementation is incomplete, still in transition, not connected
	Efficacy	PF24: Provider may make errors, EHR contains incorrect information
	Efficacy	PF32: "EHR top-down design from Government does not get trust from providers."
	Efficacy	PF33: Better to have electronic chart than the paper chart, EHR not perfect, but rich in information.
	Efficacy	PF37: Doctors see some Error in EMR/EHR, but not of significant impact
	Efficacy	PF43: Records are not organized, hard to find and time-consuming to get the right information
	Efficacy	PF45: Interoperability has not been extended to most hospitals
	Countermeasure	PF26: Hide information to avoid an abusive spouse
	Countermeasure	PF27: Patient paid out of pocket to protect privacy
	Countermeasure	PF30: Devoting more time and carefully inputting EHR
	Countermeasure	PF36: Use own private code to protect patient privacy
	Countermeasure	PF38: Patient withhold information is rare, but might occurs when with family members
	Countermeasure	PF39: Patient withhold information fearing the loss of benefits
	Countermeasure	PF42: Doctors code to protect their own sensitive and private information

Table 7-2: Preliminary Findings from providers focus group interviews

	Research Sub-Questions / New Findings in themes	Preliminary Findings
	Q.9	PF46: Government-group perceived that security protection of EHR is adequate but have a new challenge
	Q.9	PF47: Government-group thinks that verbal exchanges of information are somehow reinforced but not reduce with EHR as per the published statement
	Q.9	PF49: Legal group strongly disagree that EHR helps the government to reduce rising health cost
<b>Ch. 6 Payer</b>	Q.9	PF51: Deficiency of skillsets, integration and timely availability of implementation policy
	Q.9	PF52: Data are desensitized before available for research
	Q.9	PF53: Training for service providers is needed
	Q.9	PF54 EHR privacy protection cannot prevent leaks by humans
	Q.9	PF55: Lockbox not ready to be implemented yet
	Q.9	PF56: Gaps in national standards and provincial implementation
	Q.9	PF57: Implementation under pressure to complete as fund requires justifications
	Benefits	PF48: Professional Group has a similar assessment with government group in the government published EHR benefits statements
	Benefits	PF50: EHR could result in an extensive medical and knowledge database

Table 7.3: Preliminary Findings from payers' key informant interviews

The following table is created as a result of triangulating the preliminary findings from the 3Ps. Five significant themes (privacy to efficacy) are drawn from the preliminary findings to characterize the findings of the research results. A “+1” signifies support in contribution from the specific preliminary findings to the sub-topic under the theme. A “-1” signifies a deterrent in that sub-topic within the specified theme. The triangulated themes and sub-topics are formed by the Type 3 findings with PF from all 3Ps, the Type 2 findings with PF from 2Ps and the Type 1 (single P) findings. For example, the Types 3 findings can be visually recognized when multi-preliminary findings (PF) enlisted from the 3Ps in the table below.

Potential Findings (PF)	Theme	Privacy			Countermeasure				Benefits			Training		EFFICACY			
	Sub-topic within theme	Insufficient Protection	Genuine Concern	Add Protection	There Is Risk	Need for	Exercise Control	Withhold Information	Reduce To Get Treatment	Losing Financial	Increase Benefit	Time consuming	Need Training	Issue in Design	Trust	Efficacy / Efficiency	
	Findings Type	2B	2A	3A	3D	2C	2D	2E	1A	3C	3B	1	3E	2F	2H	2G	
1	Patients		1					-1									
2				-1													
3															1		
4			1														
5			1					1									
6																	
7				1			1										
8				-1						1		-1					
9				-1						1	1						
10				-1			1										
11				-1					-1	1							
12						1		1						1			
13	Providers				1						1						
14											1					1	
15											1					1	
16											-1			1		-1	
17													1			-1	
18											1			1			1
19		1															
20		1															
21						-1									-1		
22				-1		1											
23							1					-1					-1
24						1								1	1		-1
25							1		1								
26				1			1		1								-1
27				1							1						
28			1														
29			1	1			1										-1
30							1						1				-1
31												1, -1			1		
32															1	-1	
33												1			-1		
34														1			
35									-1								
36				1			1										-1
37												-1					
38				1					1								
39						1			1			-1					
40			1			1					1						
41			1								1						
42		1					1	1									-1
43													1	1			-1
44														1	1		
45				1											1		-1
46	Payers			-1										1		-1	
47		-1									1						
48											1					1	
49											1			1			
50												1				1	
51													1			1	
52		-1		1											-1		
53														1			-1
54				1		1											
55		1													1		
56															1		-1
57															1		-1
Total PF: each subtopic		6	8	15	8	9	3	7	3	5	15	3	8	14	2	21	
Total PF: each theme		29			27				23			11		37			

Table 7-4: Assimilate Preliminary Findings into Type 1, 2 or 3 Findings. With emerged themes

From the table above, the fifty-seven preliminary findings from this study are segregated into five Type 3; eight Type 2 and two Type 1 findings. These findings are segregated across fifteen sub-topics within five important themes.

### 7.8.1 Type 3 Findings

The five Type 3 Findings (T3A – T3E) are triangulated from all 3Ps to form the sub-topics of “adding protection in privacy”; “increase benefits, “losing financial benefits”; “privacy risk in EHR” and. “need training.” Seemingly, Type 3 finding provides a multi-angle of evidence, and a boarder view of the findings as these are opinions and attitudes are contributed by all 3Ps.

#### **T3A --- Adding Privacy Protection**

**Finding:** *Patients and providers’ ability to specify or to add privacy protection is systematically weak and limited. When facing the need for life-saving treatment, patients will sacrifice their privacy.*

Preliminary findings from the 3Ps include PF2, PF7, PF8, PF9, PF10, PF11, PF26, PF27, PF29, PF36, PF38, PF45, PF46, PF52, and PF54 with support (1) or undermine (-1), as shown in the Table above, of privacy protections. These PFs are triangulated into a Type 3A Finding.

Given that payers have had an inadequate consultation with patients and providers in the development of EHR system, the potential concerns of privacy from patients and providers were not addressed in the EHR design. With this premise, payers have designed the EHR privacy protection from data protection in the framework of workflow and technological protection neglecting actions of human hackers. It becomes a technical model of data protection of privacy rather than from a solution to a stakeholder (human) need for privacy protection. In contrast to the needs of patients wishing for the mechanism such as the ability to view their own EHRs or the capability of specifying a privacy profile in EHR, the system does not offer patients any active role in protecting their private and sensitive information in EHR. This can be triangulated with the findings that payers do not see patients as users and therefore, minimal patient consultation and needs assessment was conducted.

Patients are the highest risk group if their life is at stake [PF2, PF11] and they have specified the desire for some controls of their data in EHR [PH12]. However, to patients, receiving treatment is more important than social embarrassment, and financial loss for such providers have confirmed in their

observations [PF26, PF27], and payers acknowledged the challenges of privacy protection of patients' data [PF46, PF47, PF52 and PF54]. Similar to patients, providers have their own privacy concerns, and they have devised their ways to increase their ability to protect their privacy (using coding) as they have accessed and the ability to input data to EHR.

### **T3B --- Increase Benefits at a cost to stakeholders**

**Finding:** *While the EHR systems have resulted in some benefits, it inadvertently increased both the patients and providers worries regarding their privacy, resulting in cost and time inefficiencies. Payers' prospect on the ability to influence healthcare costs may not be materialized [PF8, PF13, PF14, PF 15, PF16, PF18, PF29, PF31, PF33, PF 37, PF39, PF47, PF48, and PF50].*

Granted that EHR system has contributed some benefits, it is not without issues. In addition to providers' welcoming the critical information found in the EHR (such as patient's medication history, allergy warnings, treatment history and drugs dispensed), payers can gather an extensive medical and knowledge database for healthcare management. With the new electronic form of EHR replacing the old paper form of the health record, the quality of drug dispensary and the work of providers have made more straightforward.

Like every new large-scale information technology project, EHR system solves some issues but also creates new problems. Payer could have conducted more consultations and developed a comprehensive design on EHR. The survey and focus group discussion shown patients and providers exercising the withholding or coding privacy information as they are worried about someone viewing the EHR data outside the circle of care for harmful actions towards them. The realization of benefits may not be as promised when EHR program was first announced. In addition to government payers' admittance that EHR implementation is behind schedule; incomplete and benefits are not fully materialized, the key informants from the legal group are skeptical on the benefits in the cost control of health care by utilizing EHR.



### **T3C --- Losing Financial Benefits**

**Finding:** *Issues of concerns in the privacy protection of EHR caused patient financial loss and providers' concerns regarding litigation and performance audits.* [PF9, PF27, PF40, PF41 and PF49].

While there are no financial gains for patients nor providers, the concerns in EHR privacy created concern and countermeasures from patients and providers. The concern regarding privacy is so critical that patients may be willing to incur financial loss and providers to incur time and effort to exercise countermeasures. From the study, patients will visit another doctor if their privacy in their medical information is violated by providers and their clinic staff.

### **T3D --- Risk Exists in EHR**

**Finding:** *The nature of digital data in EHR is a risk issue to patients and providers.* [PF12, PF13, PF21, PF22, PF24, PF39, PF40, and PF54].

Patients concerns about the risk of unauthorized access, errors, the broader exposure and faster transmission of their private information in EHR than paper-based record resulted in an overwhelming desire to control their private information in EHR. Some patients know that they are entitled to see their EHRs while other patients do not know their entitlement. Providers are concerned about the risk of the misuse of EHR by a third party outside the circle of care and patient's litigation against them after the patient saw the treatment information in EHR. Payers, on the other hand, admitted that EHR privacy protection could not prevent leaks and breaches of privacy despite the satisfaction of using a technical approach with computer applications to protect the private information in EHR.

### **T3E --- Training (Communications) Needs**

**Finding:** *Training for both patients and providers is needed. Patients were not educated on how privacy is protected in EHR system. Providers identified that EHR system is hard to navigate and operate. This gives rise to the need for training to correct the problem. Better and more open communications from payer could have identified and resolved some of the issues [PF12, PF17, PF24, PF34, PF43, PF44, PF51, and PF53].*

Patients were not informed on how privacy protection is designed in the EHR system. They only know that their information in EHR system can be sent faster and to many more providers. Given most of their experience were using paper-based healthcare record systems and that there has been a great deal of news about breach of privacy in digital data, patient's natural reaction may be to take control and exercise countermeasure to protect themselves from harm. Providers claimed that the navigation and operation of the EHR system could be difficult and time-consuming. The concerns of the above issues could be reduced with communications and education to patients and providers. In this regard, payers have not provided any consultation and training to patients other than marketing the benefits of EHR to patients. According to the providers, there was not much training on how to use the EHR system.

### **7.8.2 Type 2 findings**

Of the eight Type 2 findings (T2A to T2H) found, they are within the themes of "Privacy," "Countermeasures" and "Efficacy." Type 2 Findings are from any two of the three Ps (Patient, Provider or Payer)

### **T2A --- Privacy concerns in EHR are genuine**

**Finding:** *Both patients and providers have genuine concerns about the breach of privacy in EHR [PF1, PF4, PF5, PF22, PF28, PF29, PF40 and PF41].*

While Patients responded with a substantial agreement that they have privacy concerns across the four dimensions in CFIP model in the survey, providers expressed their concerns about their privacy in EHR through focus group

discussions. The level of concerns is strong enough that both groups have devised their action to counter the risk and implement their protection mechanisms. When compared with paper-based EHR, the risk of unauthorized access, misuse, and inaccuracies of private information in EHR. Although this could also happen in paper records, the electronic means of EHR provided a more extensive spread and instant availability of information that has multiplied the risk and extent of exposure and therefore, the impacts of the breach. Providers identifiable information is often associated with the record as input data to the EHR is tracked with their login credentials. The concerns of privacy of patients have been triangulated from different gender and different career stage groups of the patients. All show similar levels of concern.

### **T2B --- Insufficient privacy protection**

**Finding:** *EHR privacy protection does not sufficiently address patients' and providers' concern* [PF19, PF20, PF42, PF 47, PF52, and PF55].

Payers in their design of privacy protection in EHR, deploy system and technology protection. Computing security models are used to protect information security in areas of confidentiality of information, the integrity of data with its transmission, and availability of information to only the authorized users to prevent unauthorized access. However, there is a different expectation from the patients and providers. This includes misuse of their information that they have not authorized outside the prime purpose of providing immediate healthcare (outside the circle of care). The survey shows that patients have their privacy concerns and wish to have more control over the EHR data to the ultimate needs of being able to specify a privacy profile. Focus group discussion reviewed providers' concern of misuse of their data, diagnosis, and notes in the EHR for a purpose other than treating the patients. Payers confirmed that "LockBox" features are not yet implemented and that there are other modules in EHR that are still in development. Through focus group discussions, it appears that payers may not be fully aware of the privacy needs of patients and providers. Payers relied on the traditional computing system and technology model to protect the security of data and in terms achieve the result of privacy protection of data may be insufficient. Providers admitted that there

is no full patient privacy, whereas payers acknowledged that verbal exchange of information is somehow a reinforcement with the EHR, but not a replacement. Patients aware of the exposure of their private and sensitive information when they are verbally provided at a clinic, pharmacy or in the waiting room with an attending nurse or other staff. Payers claimed the standard procedure of de-identifying data before available for research. However, the author has also heard of special permission can be applied to get more information describing the dataset in research. It is potentially possible to use the process of elimination to produce personal identifiable information from a combination of single or multiple datasets.

### **T2C --- Need for countermeasure**

**Finding:** *Patients and providers do not have ways to affect the design of the EHR, the need for countermeasure is a passive way to reduce their risk [PF7, PF10, PF23, PF25, PF26, PF29, PF30, PF36 and PF42].*

In the current EHR system, patients do not have ways to influence the EHR systems as there is no patients' direct access or inputting information into the EHR system. Data in EHR is either automatically collected as a result of patient's laboratory test or manually inputted by providers. Patients obtained their EHR data normally via a request for the providers to duplicate a copy of their laboratory records or doctor's assessment by paying a fee. For the providers, they have little influence on how the EHR is designed. Also, it is perhaps unpopular for them to express their concerns about their worry of patient's lawsuits against them and the oversights from management on their productivity or evaluation from other parties.

Most patients (93%) have acknowledged the use of action (to providers) if their privacy is violated. They will also exercise countermeasure to reduce the risk of losing their benefits. It appears that payers do not anticipate any push-back or countermeasures from patients and providers as they assume that patients will be given full information to the provider when treating their illness and that providers are merely users of their EHR systems. It appears that perhaps, payers should have performed more holistic analyses before designing the EHR system and from the viewpoints of patients and providers.

### **T2D --- Exercise countermeasure**

**Finding:** *Both patients and providers have exercised countermeasure to reduce the impact of privacy breach. Patients acts outside the EHR system and providers exercise countermeasure within the EHR system [PF6, PF12, and PF42].*

As patients have no direct access to the EHR system, they can only passively perform countermeasures. Scenario questions of the survey showed that patients would hide private information, visit another doctor for same treatment and withhold information to avoid being tracked. These countermeasures are confirmed in focus group discussion with example cases such as an abusive spouse or trying to avoid paying child support. Doctors have reduced their concern of privacy with the coding of information in EHR, nurses have carefully worded the EHR data with excess information to ensure that there is no misrepresentation or misinterpretation of the information they have entered into the EHR system. The question remains will there be any way in a comprehensive EHR system to address the patients and providers concern? Perhaps, an across board training system to disseminate the EHR privacy protection's capability to providers and patients and at the same time payers need to listen to the concerns from these two stakeholder groups continually. Could there be a supplementary privacy sub-system addressing the patients and providers privacy concerns by hardening the EHR system?

### **T2E --- Withhold information as a countermeasure**

**Finding:** *The goal of patients in the EHR system is ultimately seek health treatment. When weighted between health risk vs. privacy risk, patients make a rational choice of treating of health first [PF2, PF11, PF25, PF26, PF29, PF30, PF36 and PF42].*

It is clear that patients have excised the hiding and withdrawal of their private information as witnessed and triangulated with providers during focus group discussions. However, patients will give up their privacy if they believe that their health has deteriorated. They will voluntarily disclose their private information when they perceive that they are in a life threatening situation. This is

also a validation of the Maslow's hierarchy of needs as the physiological life-threatening situation is of a higher need than the financial benefits and social embarrassment.

### **T2F --- Issues in design affects the efficacy**

**Finding:** *While some providers welcome the digital form of health records, other providers felt that in an EHR system, some basic designs are an issue of efficacy.* [PF16, PF21, PF24, PF31, PF32, PF33, PF44, PF45, PF46, PF49, PF52, PF55, PF56, and PF57].

Providers welcome the digital EHR information especially the electronic charts which can be instantly available than the finding and retrieve of old paper charts. However, their perceptions are that the EHR system solves some problems but also creates a new set of issues. Providers admit that there could be an error in EHR and that the high-speed transmission and extensive coverage of the distribution of information to recipients can be a problem. It could be difficult to correct the same errored information as there are many data backups in the system. Also, there are the concerns of design gaps in the national blueprint standards specified by CHI and provincial implementation by eHealth Ontario such that interoperability of the EHR has not been extended to many hospitals. Another issue that providers have identified is that EHR is a top-down design from government and they do not have a high-level of confidence or trust that the government can create and manage such a large scale and an extensive information technology program and develop such complicated software applications, procedures, and policies. Providers feel that security and privacy protection of EHR is the responsibility of the government but in fact, that information security and privacy protection of EHR data should be the responsibilities of everyone who comes in contact with the data. Payers perceived that security including privacy protection of EHR is adequate but acknowledged that there are new challenges.

## **T2G --- Efficiency, and efficacy**

**Finding:** *While EHR system increases efficiency and makes provider's work more manageable, the unresolved privacy issues reduce the efficacy and ultimately the potential benefits.* [PF14, PF15, PF16, PF17, PF18, PF23, PF24, PF26, PF29, PF30, PF36, PF44, PF43, PF45, PF46, PF48, PF50, PF51, PF53, PF56, and PF57].

There is no doubt that EHR can provide providers the health information much faster than the traditional paper-based health records. Providers have confirmed that critical medical information in EHR which includes: medication history, allergy warning, treatment history and drugs dispensing history being holistically helped increase the speed of a quality diagnosis and treatment plan. With the digital form of prescriptions instead of a hand-written prescription, pharmacists reported an improved quality of drug dispensing. In the backdrop of time efficiency and efficiency in data distribution, EHR that contains errors which are often seen and confirmed by providers has degraded the efficacy of the EHR system. Providers felt that it is hard to navigate manuals and difficulties in finding the right page of information. Therefore, much of the efficacy is curtailed.

Other issues ultimately affecting efficacy is the privacy risk perceptions of patients and providers resulting in the provision of incomplete data by providers in their coding of information. This reduces of the quality in the sharing of EHR data due to the many countermeasures are undertaken by patients and providers. Payers reliance on contractors and their inexperience in EHR design and implementation caused scheduled timelines of the project to be missed resulting in the slow and incomplete implementation. The unstable organization environment with several different CEOs, non-fulltime contractors and the building of EHR for the first time in Ontario influenced the efficiency and efficacy of the EHR. These issues have greatly restricted many of the planned benefits.

## **T2H --- Trust affecting the efficacy**

**Finding:** *Patients in general, trust the provider's ability to keep their data safe and private, but have concerns about the proliferation of their private data and unauthorized access. Providers do not trust the government ability to build with a top-down design of the EHR systems [PF3 and PF32].*

Trust affects efficacy and the willingness to providing clear (unencrypted) and precise medical information during the critical stage of acquisition of data into the EHR records. With patients having little understanding of the EHR systems and provider with insufficient training, coupled with their concerns about privacy have no specified channel to feedback to the payers (designers). The EHR system is not trusted for the protection of privacy. The trust on EHR capability to protect private information within its database is also weakened as many news and incidents of privacy and data breaches (including cases on the loss of EHR data by nurses and doctors) were reported by media. Providers have seen lawsuits against some of their colleagues as patients are now able to get a copy of the EHR and diagnostic assessment. Both patient and provider groups have privacy concerns that are not addressed by the payers. This limits the expected performance and quality of the EHR system.

### **7.8.3 Type 1 findings**

Type 1 findings describe the attitude and perspective of a single P. Two Type 1 Findings (T1A, T1B) were found. Type 1A related to “getting treatment” contributed from the patient’s survey. Type 1B finding is the complaints from providers on “time-consuming” in navigating the EHR system to find the needed information. As a result of triangulation and asking the questions differently, the Type 1A and Type 1B findings are a subset of T3A and T3E. The following will be a brief description of these two findings.

#### **1A --- Reduce benefits to get treatment**

**Finding:** *Patients will opt for getting treatment and forego the benefits [PF8, PF9, and PF11].*



Patients are rational. Getting treatment for their health problem is the primary purpose when visiting a doctor. When faced with severe illness, patients will forgo their benefits whether it is a financial loss or social embarrassment.

### **1B --- Time consuming, therefore, needs training**

**Finding:** *Providers have reported difficulty in using EHR, especially trying to find the required information through the complicated menu. Training will be a solution to increase efficiency and efficacy [PF17, PF30, and PF43].*

While payers perceived providers are not IT savvy, providers have little involvement in helping the specifications and the presentation of information in EHR. This results in providers having a lack of familiarity with EHR system which extended to time-consuming searching for information in the EHR system. It is believed that proper training and presentation of the capability and limitation of EHR systems to the providers will help resolve the issues.

## **7.9 Five Themes Established from Findings**

The following sections discuss the five themes that have been identified based on the triangulation of sub-topics. These themes are Privacy; Countermeasures; Benefits; Training, and Efficacy.

### **7.9.1 Privacy**

Privacy in EHR is a real concern not only to patients but also to providers. The reason for a patient to hold on specific health and sensitive personal information as private because the exposure of such brings along the detrimental effect of loss of benefits: financial, social or emotional exposure, for example, a sexually transmitted disease, substance abuse or terminal illness. Despite the difference in age (PF3) and genders (PF4), there is a consensus from patients that the privacy protection in EHR is grossly inadequate as evidenced with the survey

results across all four dimensions of CFIP (Preliminary Findings - PF1, PF3, and PF4). These concerns are a reality to patients as evidence from the survey and the validation of patient's action in taking countermeasures. Patients prepared to take action to the extent of changing doctors and taking legal action (Scenario-SSWC) against their service providers should their private information in EHR is be shared with individuals outside their circle of care.

Other evidence in this research support the real concerns of privacy in EHR, including the agreement of the service provider to follow privacy exposure issues. These include their reception area and the verbal exchange of information that can be overheard [PF19], no full patients' privacy [PF20] and unauthorized access [PF22], Errors do occur in EHR [PF24, PF37]. Payers have a different view of the verbal exchange of private information. They claimed that the protection of verbal exchange of private information is somehow reinforced in the EHR system, but the risk of exposure to the third party is not reduced [PF47].

As recently as Q4 2017, the author has observed that the ECG (Electro-Cardiogram) machine installed within a computer in a laboratory is still running an obsolete, unsupported and security vulnerable Microsoft "Windows XP Professional" operating system. Windows XP Professional systems were declared obsolete with no further security support from Microsoft Corporation as of April 8, 2014, which is after 12 years in service (Microsoft 2014).

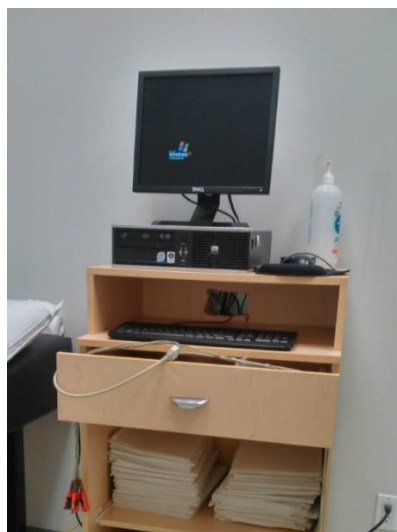


Figure 7-5: ECG machine using obsoleted "Windows XP" operating system

It is this overhearing of private information such as patients' conversation with a nurse or medical receptionist during the computer entry of EHR information into the system, and the operation of computer systems without adequate security installed, which gives rise to patients' beliefs that EHR system is weak in the protection of their private information. As patients encountered the EHR system at service provider's location, the perception of how patient's privacy protection is not protected can be observed relatively easily. In general, patient answering questions in clinics are easily heard with names, date of birth, home address and phone number be heard if listen attentively by a bystander in the waiting room.

It must be pointed out that service providers are now slowly finding ways to protect patient privacy. Although in many providers' medical reception areas, there are still the overheard patient-receptionist dialogs, some providers are slowly taking a step to reduce such impact. The photograph below shows how a clinic is minimizing the overhearing of private information between the patient-receptionist dialogs. The sign directs the person next in line to stop proceeding to the reception counter until being called, thus affording a distance to prevent overhearing of information.

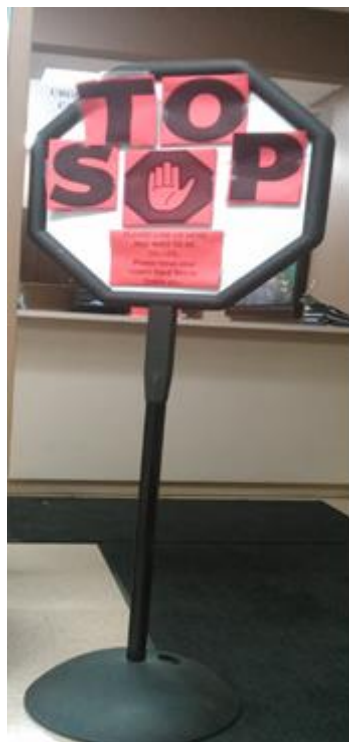


Figure 7- 6: Providers try to reduce over-hearing of patient's conversation

The separation of the patient at the reception counter and the next person in line makes it difficult to overhear the patient's conversation at the counter. It would be interesting to explore in future research that if such measure is a result of providers' awareness of privacy concerns out of the worry in their own privacy in EHR.

Similar to patients, providers are also concerned with the illegal access of their private information by hackers or unauthorized third parties. In contrast, payers have little concern for privacy in the EHR system that they have implemented. Payers considered patients' need as secondary, and providers are not viewed to be information technology savvy. Questions were raised in Chapter Two, "Are patients being given appropriate consideration in the patient-centered EHR system?" Payers make claims that the EHR provides many benefits in the quality of treatment to patients. However, they do not view patients as playing an active role in the EHR system. However, when sufficient numbers of patients withhold information, the completeness and effectiveness of the data in EHR system become questionable. Payers believe service providers are the primary users of EHR, in the author's assessment and judgment, service providers are only the technical users of the patient information in EHR system and inputting the patient's health records into the EHR, therefore, performing the proxy function on behalf of the patient.

Factors that gave rise to patients and providers concern about privacy in EHR could be stemmed from payers not involving providers in EHR design and furthermore, not conducting consultation with patients to uncover their concerns about EHR. The perceptions from the payers during the key informant interviews are that providers are difficult to solicit regarding systems and operations requirements, as they are not technical enough to have an active discussion about system design.

Payers perceived that patients are secondary as EHR is merely a tool for the providers to treat the patients' illness. This ignores the facts that patients are the primary stakeholders that have the most to gain and risk (medical and benefits) from a functional EHR. Payers perception also undermines that patients are the owners of their medical information in a medical record, as affirmed by the Supreme Court of Canada.

Why the inadequacy of privacy protection in EHR? Through triangulation of different findings from this research, a plausible explanation of patients' privacy concern stems from the evidence that patients are considered secondary by payers. Payers consider service providers as users of EHR and that patient's participation and corporation in the EHR system is a given since patients depend on the provider to provide diagnosis, treatment, and referral. Patients are not the main stakeholders in EHR even though patients are the owners of their information in EHR system. With these assumptions, payers have little consultation with patients to assess patient's needs and concerns about the EHR project. Much information published on EHR to the patient is of marketing nature of describing the benefits from the payers perspective. Aside from the unstable organizational and design environments, given a massive EHR initiative with software implementation being the main technical backbone capturing and transmitting sensitive and private data, there is a lack of formal inputs from two of the primary stakeholders. These stakeholders are the patients and providers. In the opinion of the author, the above adverse conditions contributed to the patients and providers privacy concern in the EHR data. This leads to subsequent countermeasures to protect their privacy. With such countermeasure, the efficacy and efficiency of EHR implementation are diminished.

### **7.9.2 Countermeasures**

Countermeasures are a response to perceived risk. Perception becomes a reality when risk is believed to be real by patient or providers. A critical realist will try to expand the vision to uncover any ordinarily unobservable event that may influence a person's perception. To many patients, the easiest way to change the outcome of perceived reality than to spend the time to find out the fact and truth upon which perceptions can be changed. The patients will devise and execute countermeasures to reduce their risk and more importantly, the impact of loss or adverse effects suffered.

A systematic sharing of information and the risk of who controls the access can be uncomfortable to patients and providers as there are unknowns and a loss of

control to favor their required protection. Sharing of information facilitated by the EHR system design is one of the fundamental enablers of the benefits of EHR. However, both patients and some service providers perceived risks in sharing their private information, especially by design, the EHR is widely being distributed in a network. Not all information recorded in the EHR should be shared especially some private and sensitive medical information that, if exposed to a person with unjustified reason, could result in detrimental consequences to both the patient and the service provider. According to Griener (2005), the traditional physical paper records of health information cannot be distributed as widely with and as many copies instantly available as the digital EHR. Therefore, the impact of a privacy breach on a paper system is lower than the EHR. Another issue is the transfer of the authority from a provider involved in deciding who gets access to their paper record of health information to a system decision based on pre-determined factors of who gets the access to the health record in their custodianship (Griener 2005). This removal of local decision-making over who gets access to the electronic health records gives rise to the privacy concerns of the patients and providers as each group has the right to control and implied ownership of private information placed in the EHR system.

What causes patients to perform countermeasure? One percent of patients will not disclose any private information regardless of their emergency situation, according to the survey result. Very often, patients are faced with the balance of their objectives between seeking medical treatment to cure their disease and the protection of their private and sensitive medical information. This research found that most Ontario patients would disclose to various degrees their private information in return for proper treatment. When sickness worsens, 86% of patients will give out private information (WIW). Patient withdrawal of information was evidenced in the survey (SDWE) with nine percent of patients not telling providers sensitive information until they find out the seriousness of their condition. It appears that patients exercise withdrawal of information if monetary benefits are of concern or there is potential for emotional or social embarrassment. There is a shift of behavior with patients resist in giving information to nurses and pharmacists rather than to the doctors. Nurses and

pharmacists agreed that they often see patients withholding information by walking away [PF25], [PF26]. This is in contrast to doctors only seeing patients withholding information when with family members [PF38].

For the providers, there is a very different risk of exposing their private information in EHR. The exposure of a provider's private information to peers, who often are otherwise authorized to access as the EHR is a role-based protocol to gain access to the system. This could result in biased opinion towards the reputations of providers. Since most providers are paid by the provincial health insurance plan (OHIP), they are not able to opt out of the EHR. Therefore, unlike the patients who can walk away and see multiple doctors or provide inaccurate information, providers must find ways to countermeasure their risks in EHR by adapting and exploiting the available venue to code information that they would like to keep private. Nurses and pharmacists take extra time to ensure information written into EHR is detailed and accurate to the extent in justifying their actions in giving out the care. As a result of such countermeasure, the efficiency and effectiveness of EHR are degraded.

The payers' view is that EHR by design is to be widely shared by authorized users without the need to check if they have reasons for access. In case of emergency and for flexibility, this allows a quick assembly of resources (EHR data) and needed medical expertise to efficiently join the care group and provide timely assessments via electronic access without the high cost of on-site travel. It is also a useful way for public health management to recognize an outbreak of a significant disease in the early stage in addition to improving the management of the cost of healthcare.

A dialectical discourse on the countermeasures above --- to understand the above countermeasures from the patients and service providers, one can use the dialectical model of the thesis, antithesis and synthesis from Fichte (1794) to attempt to gain insights to the behaviors in actions. Given the thesis of privacy concerns perceived by patients and providers, the antithesis that patients have made is to countermeasure their concerns including non-disclosure of sensitive information during annual checkups, paying out of pocket to doctor hop to another doctor who is not participants of the EHR or seeking an out of country

medical treatment. The antithesis for the service providers to resolve the conflict is to encrypt sensitive information with codes that only they can understand. Therefore, reducing the exposure of their sensitive information even if the information is widely accessible by design to multiple users. A possible synthesis to resolve the situation would be an action by payers to ensure the privacy protection of EHR data by hardening the privacy protection mechanism and holistically addressing the breaches from both the technical and human hackers with the implementation of stronger policies, procedures and all-around protection. Payers need to acknowledge the privacy needs of patients and providers as a starting point and start to resolve the current status.

### **7.9.3 Efficacy**

According to Oxford Living Dictionary and Cambridge Dictionary, Efficacy is defined as the ability to produce a desired or the intended result. In the EHR program, efficacy can include efficiency, adequacy, and competence. This study focuses efficacy from payers claimed benefits and objectives and reviews if the design and implementation of EHR system can produce its desired or intended result.

A good and robust system design, process and procedure usually result in better efficacy. There are issues in the EHR system that are detrimental to its efficacy. Firstly, inadequate and weakness in the design of privacy protection. The problem in this area is payers could have collected the additional design specification if they have conducted the necessary consultations with patients and providers. Such design specification requirements could have addressed the patients' concerns [PF1, PF6, PF12] and incorporated patients wish to have some controls over the privacy protection of EHR from reviewing, specifying what information to protect and to the extent of specifying a privacy profile. By using design restrictions, policies and procedure to address providers concerns (PF22, PF28) of unauthorized access by other medical staff or hospital administrator could have been addressed. People who are outside the circle of care or have no business relationship with the patient should not have access to the private information of patients and providers. Payers' attitude further



worsens this unauthorized secondary access as payers believed that privacy protection is sufficient in EHR system. Payers accept that privacy protection cannot prevent human leaks and the verbal exchange of EHR information is not reduced which is in contrast to the claim in their publications [PF46, PF47].

Secondly, the fact that EHR architecture and design is based on a top-down model creates specific issues. There are the gaps in national standards and provincial implementation as cited by the payers [PF52]. The top-down hierarchical stewardship and leadership is also an issue. Canada Health Infoway (CHI) designs the architecture. Provincially, The Ontario Ministry of Health (MOH) is responsible for the leadership and stewardship of the EHR project within the province. A third and independent crown corporation, eHealth Ontario performs the design and implementation based on the requirement from CHI and directions from its immediate supervisory organization, the Ministry of Health. There are opportunities for miscommunications and misunderstandings. At the user level, providers did not have much trust in the EHR project as they were not involved in helping develop requirement specifications, and the system is not a bottom-up design which could have addressed many of the providers' concerns [PF 32]. A robust capability in human resources allows ultimately, efficient operation and the ability to resolve challenges arising from the operations of the EHR system. The efficacy of EHR program relies on the payers to hire capable and skillful designers and implementation team to release the deliverables of the program. From the evidence collected in this study, there are several concerns raised. First, there is a lack of skilled professionals in this project. Payers have revealed that there is a deficiency of skillsets in their workforce [PF47]. This results to the hiring of external contractors and consultants who may be staying only on a specific stage of the project, and there is reduced likelihood for the eHealth Ontario to retain the sufficient knowledge for proper system integration. Second, the effects of the change of leadership within eHealth Ontario, the falling behind in setting policies before design and implementation caused a "best effort" than a "best design and built" situation. This ultimately lead to missing the published schedule of deliverables. As discussed in Chapter Six, many designs were crafted without a design policy and detail specifications.

Plans were modified after the effort of chasing, finalizing and receiving the detail design directions and specifications. A “cart before the horse” scenario was described in the interviews. In the opinion of the author, this lack of skillsets, the use of many contractors and consultants, resulted in the disjointed and less effective design and implementation.

Thirdly, the lateness of the deliverable created program integration delay and reduced the expected efficiency after integration. Late deliverables placed pressures on the design and implementation team. This invited the release of a not fully completed deliverable for justifications of funding. Lastly, the lateness of implementation, in many cases, incurred extra costs which diminished the organization’s ability to obtain additional resources or higher paid expertise. The analogy of “repairing the car while it is running at high speed” scenario was discussed in the KII interview.

Trust is one of the constructs in the research framework of this study. Whether it is human to human or human to system interactions, trust modulates the outcome of the EHR efficacy regarding patients’ willingness to disclose their sensitive and private information in the EHR system. It is a modulating variable in the research framework in Chapter Three. Providers diminish the efficacy of the EHR system as they do not trust the EHR system for its privacy protections. Patients largely lack an understanding of how the EHR could protect their privacy. The trust level is low especially the impact of a breach of private information that could have detrimental effects on the patients financial or emotional well-being. To the providers, a privacy protection mechanism is needed to protect their patients and themselves from litigation and unwanted audits. Both the patients and providers’ countermeasure reduce the time and financial efficiency financially resulting a lower efficacy of the EHR systems. It negates the many intended benefits of the EHR system.

Efficiency is a major benefit of implementing EHR. With time-efficiency, laboratory results in EHR can be made available faster with the use of electronic means. Resources-efficiency can be made possible by reducing duplicate procedures as EHR contains the history of all laboratory, medications and diagnosis results. Sharing-efficiency is achieved with high-speed security

protected network for EHR data distribution. To the patients, quality of treatment and time efficiency in the treatment of illness can be improved. To the payers, cost-efficiency and data-acquisition-efficiency can be achieved with digital information in EHR that can be acquired and transported to the requested service provider faster and more accurately when compared to handwritten paper records. Digital data allows quicker computing processing in the analysis and pattern recognition for public health management. All of the above benefits and desired results are part of the components of the efficacy of EHR in achieving the intended effect.

In the area of Time-efficiency, providers agree that generally, EHR will increase efficiency and makes their work easier [PF14]. The availability of critical information in EHR includes medication history, allergy warning, treatment history and drugs dispensary (taken) history in addition to the usual demographic information and diagnostic images of the patient. The presentation of holistic health information in an EHR helps doctors arrive at a quicker and a higher quality diagnosis.

Due to privacy concerns, patients have exercised countermeasures by withdrawing information, giving incomplete information or even walk away in the middle of providing EHR data to the service providers. This creates time inefficiency as EHR record is incomplete or the record is aborted during inputting. The need to share service providers' sensitive and private information reduces the time efficiency of EHR. To the nurses and pharmacists and doctor's concerns, they have devoted more time and carefully inputting data into the EHR [PF17], [PF30], [PF36]. Another time deficiency reported by the doctors is that they have spent much time navigating to find the right information in EHR. This reduces the time efficiency.

Resources-efficiency, in this research study the availability, completeness, and accuracy of the contents in EHR are examined. According to the pharmacists in the focus group discussion, EHR will reduce medical errors and improve quality of drug dispensing [PF15]. Providers also reported that information in the EHR system had provided essential and sometimes critical information [PF18] for a quality diagnosis. However, EHR data may be inaccurate, incomplete or coded

for privacy protection. Both the payers and providers have confirmed that some EHR modules are not yet implemented [PF16, PF55] these reduce the contents available in EHR and therefore reduces the usability of resources (resource efficiency is reduced). These inefficiencies reduce the efficacy of the EHR.

Cost-efficiency would be a benefit if EHR can help reduce duplication of a lab test, improve time to diagnosis and shorten the time of patient's sickness as such it also reduces the duration of sick leave from work. However, the implementation of EHR projects has a cost overrun as described in Section 1.6 and Section 6.8.3. Both the government group and professional groups of payers have a similar assessment that EHR will help slow down the rising health-cost, but the legal group in the key informant interview disagrees that EHR will help slow rising health cost. They were concerned about the costs to operate and maintain the EHR system, and the deficiencies in EHR will not prevent any cost reduction.

Data-acquisition efficiency is a result of digitizing and standardizing the format of EHR with the designed capability of sharing the records across a high-speed computer network. The storage of EHR and the ability to quickly assemble and access these records result in an extensive medical and knowledge database. The positive impact of data-acquisition efficiency allows efficient management of public health and medical research. Conversely, an efficient data-acquisition of EHR created the vulnerability of illegal access and hacking of the private and sensitive information of the patients and providers. The digital storage of EHR in a portable media such as hard-disk storage has been reportedly lost on various occasions.

Trust affects the efficacy of EHR. When both the patients and providers have doubted the EHR system as found in this research study, efficiency and accuracy of EHR will be reduced as countermeasures were launched. One of the reasons for patients not trusting the EHR is their lack of understanding of how EHR can protect their privacy. Providers do not trust the EHR as their information is widely available in a network and potentially shared by many other users or regulators who might have access to the system. This lack of trust in the EHR system from the patients and providers is further reinforced

with the reported on the loss of computer hard-disk which contains thousands of EHR information.

#### **7.9.4 Benefits**

Benefits are the cornerstone of EHR project as payers advertised and claimed that the implementation of EHR is of great benefit to patients. Does the implementation of EHR fulfill the stated benefits as claimed by the payers?

For the patients, EHR may have increased some efficiency and convenience in not having to wait for paper records, but overall it appears that the EHR system took away more of their privacy and reduced patients' level of comfort and enjoyment of their existing benefits.

From this research study, patients have fundamental concerns about privacy protection in EHR. They would want to keep their privacy as much as possible and only disclose private information in EHR, in return for better treatment when their illness is worsening. As evidenced by the preliminary findings (PF8, PF9, PF11), most patients will disclose private information to treat their worsening sickness. However, when the illness is not a significant concern, patients may behave defensively, exercising countermeasures to reduce any impact of privacy exposure. The stated benefits of EHR in areas of accuracy and completeness will be compromised as patients intentionally holding information back from the service provider. The same effect happened when providers protected themselves from coding and hiding information in EHR. This causes a less accurate EHR of patient conditions and descriptions of illness. The primary benefit of sharing EHR information among providers and the public health department is reduced when less accurate, and the less comprehensive patient information is available to share. An incomplete and less precise EHR will increase the likelihood of other service providers conducting more diagnostic tests and requiring extra examination time in the course of treating patients. This causes a reduction of EHR benefit due to inefficient use of time and financial resources in treating the patient's illness.

Other benefits were not explicitly explained to the public but are of importance to the government payer group (Gov-GP). This includes the cost controls to stem the growth of health expenditure, the ability to explore an extensive database of EHR transactions to assist in public health planning and control of epidemics with readily available digital information as well as the capability of sharing the EHR rapidly among health departments and experts. By not addressing the patient and provider's privacy in the design of EHR, payers cannot realize the full slate of potential benefits. Although the government group (Gov-GP) and the professional group (Pro-GP) agree (4.3 out of 5 in Likert Scale) that stated benefits could be realized, the legal group (Leg-GP) is skeptical of the benefits. This is especially so for cost control [PF49].

#### **7.9.5 Communications and Training**

The elements of training and consultative communications to stakeholders and users (patients and providers) to establish a specification requirement are a vital part of the EHR project. However, these two elements have not been fully implemented in the EHR project. Without a consultative and communication process with patients, payers will not be aware of the privacy needs or believe that patients and providers would exercise countermeasures. This has resulted in the diminishing the intended operational benefits of EHR.

Payers believe that the percentage of participation (an indirect indication of acceptance of EHR) of the patient will be high. Also, since service providers are paid from government funding under the OHIP, providers' participation in the EHR system would undoubtedly be high as their fees are controlled and paid by the government. These perceptions give way to the issue of lack of communications and training. Without proper consultation and participation from the patient group, the resulting EHR systems and design will be highly unilateral based on the national blueprint whereas the provincial requirement specification, especially patients and providers privacy concerns, are missing.

There is a vital difference between participation and acceptance of the EHR system. One can analyze and conclude that although participation rate may be

high, patients and providers can reduce their acceptance to the EHR system by modifying their behavior while participating in the system. Thus, the result of the action from patients and providers exercising countermeasures while participating in the EHR systems. This result in a reduction of the planned benefits and the expected efficiency of the EHR program.

Communications and training, from payers to providers and patients, are the keys to resolving the issues. Through consultative and on-going communications, payers would realize who are the owners of the respective parts of information in EHR. Payers would understand and implement the necessary design to satisfy the critical needs of privacy protection for the patients and providers in the EHR system.

Without a consultative communication and comprehensive training to patients on how and to what extent that the patient's privacy in EHR is protected, the patient has little chance to be comfortable with the privacy protection implemented in the EHR system. The same happens to service providers when they are not being trained on how the EHR system can protect their privacy and address their worries such as oversights organizations using EHR to audit or evaluate their performance.

Further examination of this trust can be supported by Preliminary Finding, PF38 showing that patient withholding information from the doctor is rare. The patient's trust is changed when some of those patients have a fear of loss of benefits, as indicated in [PF39].

Through a process of elimination, it is likely that this distrust by the patient is towards the EHR system rather than to the doctor. This distrust by the patient can be found as evidence supported by the findings in the payer's key informant interviews. There is a lack of education and communication between payers and patients. Also, payers perceived that EHR information could be inputted into EHR systems by service providers, or automatically uploaded from laboratory or drug dispensing programs when patients visit medical facilities. It appears that payer does not rely on much input from patients but expect the service providers came up with a diagnosis and treatment plan even if patients did not provide complete information.

One can believe that patients could increase their trust in the providers and payer if they have more exposure and understanding on how the EHR is used to increase their benefits and protect their privacy.

Through the key informant interviews, payers view service providers as non-technical and left with little consultation. Training acts both ways of informing the patients and providers about the understanding of EHR; it also provides a way for the payer to receive input and concerns from patients and service providers. Obtaining stakeholders' input and their concerns is critical to any large-scale initiatives such as EHR system.

## **7.6 Summary**

This chapter presented an integrated analysis and discussion of the results provided in previous chapters. The foundation question if patients and providers have genuine privacy concern is confirmed. Preliminary finding (PF) are triangulated to form Type 3, 2 and 1 Findings that lead to the emerging of five themes from privacy, countermeasures to training. The discussion in this chapter suggests that payers need to make a considerable effort in understanding the privacy needs of patients and providers. Payers also need to gain the trust of the patients and providers and thus reduce the privacy concerns and the associated countermeasures in EHR system.



## **Chapter 8 Research Questions and Conclusion**

### **8.1 Introduction**

This chapter summarizes the findings for the research objectives, the research sub-questions and the central question this study. A description of the contribution of this research its limitations is provided. The chapter ends with a conclusion and a reflection citing the challenges and success in the discourse of this research.

### **8.2 Revisit the Research Problem**

Before 2002, paper-based health records were commonly used by service providers. Hardcopy from of X-rays, ultrasound images were carried from laboratory to doctor's office by patients with the control of health information in the hand of the patient and providers. The introduction of EHR created paradigm shift with a wide range of impacts. EHR are vulnerable to security and privacy risks that have led to concerns from patients and providers. EHR data can be distributed instantly and simultaneously accessed at multiple locations which multiplied the impact should a breach occur. The custody of health records changed from provider to payers' EHR repository system which created the needs of privacy control from both patients and providers groups. These two groups exercise countermeasures which reduces the efficacy of the EHR system. Three groups of stakeholders (Patients, Providers, and Payers - 3Ps) are interrelated affecting the successful implementation of EHR system. Until one understands the attitude of these three stakeholders in their perception of each other's role and the privacy protection in EHR system, achieving of the objectives and the benefits of EHR will remain unfulfilled.

### 8.3 Research Objectives and Findings for Research Sub-Questions

Nine research sub-questions were set out in Chapter Three to aid the research objectives that in turns, guide the presentation of various findings in the exploring and understanding of the primary research question.

**Research Objective 1:** To examine the CFIP model to see if similar concerns are voiced by patients in Ontario, Canada versus patients from the USA.

*Sub-question 1: What level and the types of perceived privacy risks, (e.g., excessive collection of data, unauthorized secondary use of data, improper access of data and errors of data) are of privacy concern in EHR implementation?*

This sub-question has found that patients have strong privacy concerns on three of the four CFIP dimensions with top concerns in the “Unauthorized Secondary Use” of data. The finding confirms that patients have genuine concerns about privacy, and when their concerns materialize some exercise countermeasures. The attitude of Ontario patients aligns with a similar study in the USA. In the dimension of “Too much collection”, patients’ responses exhibited a bimodal result showing that similar quantity of patient is agreeing and disagreeing that there is too much collection of private information in the EHR.

**Research Objective 2:** To assess if patients will trade-off benefits with privacy protection.

*Sub-question 2: How willing are patients to give out sensitive and private information to service providers when their medical condition has deteriorated?*

This study showed that patients progressively tradeoff their privacy if they perceive their condition is deteriorating. Half of the patients will volunteer their private information when they are in emergency department regardless of the seriousness of their illness. Progressively, one-third more will do so if sickness is worsening and another 6% more if they are in a life-threatening situation. This result can be supported with Maslow’s Hierarchy of Needs as it is a physiological need over safety and security needs (financial security).

Furthermore, patients will be willing to provide private information even if it means that a result of social embarrassment (love and belonging).

**Research Objective 3:** To examine if patients trust their providers' ability to protect their private information in new digital EHR

*Sub-question 3: Do patients think that providers can keep their data secure and private?*

This study found that half of the patients surveyed still believe that provider can keep their data in their clinics and hospital (with a copy to EHR repository) private and secure. However, there are less than one-fifth of patients do not agree that provider can keep EHR data secure and private. About one-quarter of patients do not have an opinion on this question. It could be that the patients have not thought of this area of concern or they have not come to an opinion yet. It could be the fact that on the one hand, patients trust the providers with their practices and procedure, on the other hand, there have been frequent leakage and loss of EHR reported in the media, and as such, some remain skeptical.

**Research Objective 4:** To examine assertion from the literature that female is more concern with privacy than male.

*Sub-question 4: Is patient's gender a factor influencing the level of privacy concerns?*

This research found no difference in gender on three of the four CFIP dimensions except the "too much collection" dimension. More female respondents (33% female vs. 24% male) are less concerned that there is "too much information collected in EHR." In the areas of privacy in EHR literature, this result is in contrast to published research from Frost *et al.*, 2014; and Walrave *et al.*, 2012, which suggested that females are less likely to give out private information.

**Research Objective 5:** To examine other demographic characteristics that might affect patients concerns about privacy.

*Sub-question 5: Is patient's age group or career stage a factor influencing the level of privacy concerns?*

This study showed that there is no career stage (used to enumerate age indirectly) difference across the privacy concerns of “Error”; “Improper Access” and “Secondary Use” in the CFIP dimensions. They also respond with a high score (97% or above on the category of “agree” that there is a privacy concern. However, in the “Too much collection” dimension, the percentage of disagreeing, agree and undecided in the response are all similar with one-third scored for each of these three choices. This pattern is similar (consistent) among all three career stages, suggesting that regardless of their age, they have similar attitudes towards privacy. The result from scenario survey showed that patients would progressively volunteer their private information if they perceive that such disclosure will result in a better quality of treatment. A potential hypothesis could be that Ontario patients might believe that even when a provider collected more private information on them, it is for the quality treatment of their illness. Further study of this hypothesis is needed to understand the score in this particular dimension.

**Research Objective 6:** To find out the spectrum of control patients want to have in EHR

*Sub-question 6: What level of information access and control do patients want to have over their private data in the EHR system?*

As a confirmation of patients' genuine concern for their privacy in EHR, the behavior and the willingness of how the patient would like to control their private information is assessed. Approximately 95% of respondents would like to have some control of their EHR data ranging from able to login to their EHR to check the accuracy of their private data, to the creation of lockbox, and ultimately, specifying a privacy profile controlling which item and who can see their data

**Research Objective 7:** To assess providers concerns regarding issues that affect the quality of treatment and to triangulate this worry against patients' concern.

*Sub-question 7: What are providers concerns on EHR systems?*

The primary job of providers is to perform quality treatment to patients and helps a speedy recovery of the illness suffered by patients. EHR system promises to help to achieve these goals with a complete and holistic view of patients health records and histories of diagnosis. Providers have the following concerns that could reduce the efficacy and capability of EHR to achieve its promised goal. They are: (a) Patient withholds information or walks away when visiting the provider. (b) The verbal exchange of information can be overheard. (c) Based on the providers' experience and opinion, there is no full patient's privacy. (d) There is some distrust of the EHR system as it is a top-down design and is built and run by the government agencies. (e) EHR solves some problems but also creates new ones. (f) Providers felt that it is time-consuming inputting data into the EHR. (g) Information in the EHR is hard to find. In addition to studying the attitudes of providers, the above concerns are used to triangulate the findings and countermeasures from patients.

**Research Objective 8:** To assess if providers have their own privacy concerns as they also give out their private information to the EHR system and if providers also perform countermeasures.

*Sub-question 8: Do providers have privacy concerns in EHRs as they also placed their personal identifiable information, diagnoses, and notes in the EHR?*

This research showed that providers have the following concern related to their privacy protection in the EHR system. They are: (a) There is a privacy concern about the secondary use of information against providers. (b) Patients can have open access (via a request for a paper copy on EHR or seeing the EHR information online with laboratory report) on the diagnosis of providers' part of EHR causing misunderstanding or suspicion of treatment plans. (c) There is concern about vulnerability to legal action as EHR may expose doctors variations in practice. (d) There is an opportunity for unauthorized access to EHR information from other medical personnel outside the circle of care. (e)

There is a concern about using EHR to evaluate providers productivity or performance. The findings also confirm that providers exercised countermeasures to reduce the risk of the above and the impact to them in the event of a privacy breach.

**Research Objective 9:** To determine if challenges from payers would be the reasons for patients and providers privacy concerns

*Sub-question 9 What are the challenges and concerns from payers in their implementation of EHR?*

From this study, the following challenges have been identified: (a) There is a deficiency of skillsets resulting from an imperfect integration and delay in implementation. (b) There are gaps in national standards and provincial implementation resulting in different and sometimes contracting demands and needs of the EHR program. (c) The implementation of EHR modules is under pressure to complete as funding requires justification. (d) Payers perceived that security protection of EHR is adequate but have new challenges such as the hacking of now digital information. (e) The lockbox and other modules are not complete and therefore not implemented, resulting in a lower level of privacy protection and benefits of the program. (f) eHealth Ontario experienced too many leadership changes and a shrinking of consultant resources which resulted in an unstable environment. (g) There are cases whereby policies are not ready to meet the needs of design and implementation requires. Often, a later policy during EHR implementation forces the design to do their best in guessing the policy resulting in a sub-standard quality in the implementation.

#### **8.4 Overall Findings from the Research Sub-Questions**

The research sub-questions demonstrated that both patients and providers have genuine concerns regarding privacy and engage in countermeasures. Also, payers misperceived patients as an unimportant stakeholder and viewed providers as being technologically unsavvy. This resulted in a technical

solution of EHR without the consideration of human needs, and these solutions failed to address the privacy concerns of patients and providers adequately.

Confirming that patients have genuine privacy concerns in EHR is important. It is essential to establish a solid foundation for the subsequent exploration of the constructs in this study. Patients ranked the unauthorized secondary use of their EHR information as the top apprehension from the four alternative CFIP dimensions of privacy concerns. Patients' willingness to provide information is influenced by their trust that service providers can keep their data secure and private and also to their perception of how severe their illness is. Patients launch countermeasures to reduce impact and avoid risk entirely by withholding private information. Patients assert their control: by withholding information from the provider, by asking for lockbox in EHR, and ultimately, would like to have a privacy profile to stipulate who gets access to which items of their private information in EHR. Additionally, patients exercise countermeasures such as changing providers, complaining to providers and taking legal action against the providers in cases of privacy breaches.

By studying the providers' experience, concerns, attitude, and actions towards EHR, this study revealed many insights regarding patients' concerns about privacy. As the initiators, designers, and implementors of EHR system, payers' attitude, actions, and their organizational environment influence the patients and providers privacy concerns.

This research explores the challenges of payers in their implementation of EHR with the following findings: (1) Payers perceived that patients are secondary and no attention was given to patient's privacy concerns. As a result, payers felt that technical protection of privacy in EHR is adequate. Payers agree that EHR privacy protection measures do not prevent human leaks or data hacking. (2) The implementation of EHR system is behind schedule, and that lockbox features have not been implemented, thus reducing the efficacy and benefits of EHR. Other challenges to payers include (3) Gaps in national standards and provincial implementation. (4) Unstable leadership (changes) in eHealth

organization. (5) There is a lack of designers' skillsets in integration and the lack of consulting resources. (6) Design and implementation policies are not available when needed, and (7) The benefits of cost control from EHR are below expectations.

## **8.5 Findings for the Primary Research Question**

The primary research question is formulated to study the following constructs: stakeholder's attitudes, perceived risks, sharing and distribution of sensitive and private information in the EHR system.

The primary research question is: *“What are stakeholder's attitudes and the perceived risks surrounding the sharing of private and sensitive health and personal information with healthcare providers and potentially having the information distributed across the health system?”*

The findings of this primary question are that patients are apprehensive about EHR and they perceived many privacy risks as discussed below. Patients have significant concerns with the sharing of private information with providers, and they worry about having their sensitive information distributed across the health system. By expanding the scope of the central question; it is found that providers shared similar privacy concerns in their perceptions of the risks of unwanted access resulted from the sharing and efficient distribution of providers' data.

The EHR risks to providers include open access by patients that may initiate litigation against them, by oversight (and licensing) organizations in conducting performance review and audit of their work which may reveal biased and targeted perceptions of their practice. Providers also need to protect their suspicion on a patient's unconfirmed or unrelated, but potentially serious medical condition outside the current illness under treatment. Providers devised their own private coding of their medical notes to combat the unavoidable access by others to ensure that their medical notes even accessed, are encrypted



preventing understanding of their private contents. The inter-relationship of these 3Ps and the countermeasures from patients and providers created a deficiency in the efficacy and diminished the planned benefits of EHR.

The sharing of information expedites the benefits of EHR. However, both patients and providers believed that EHR increased privacy risks when health information changed from paper-based to digital format. According to Griener (2005), traditional paper health records cannot be distributed as widely with as many copies instantly available as the EHR. Therefore, the impact of a privacy breach on paper record is under control and lower than that in the EHR system.

Patients have expressed significant concerns about their inability to control their private data in EHR. When EHR replaces paper records, the transfer of the custody and control of health record moves from providers to payers who control the repository of EHR system. This shift of the custodianship removes a provider's ability to decide, for the benefits of the patients, who might be allowed access to the health record under their custodianship. EHR gives rise to the privacy concerns of patients and providers as each group has previously enjoyed the implied ownership and the right to control their own private information placed in the paper-based health record. This absence of custodianship induced the need for control that results in countermeasures to reduce the impact of a privacy breach.

The findings relating to efficacy showed that (1) Patients withhold information and provider coding practices created incomplete or partially unreadable information in EHR. This becomes a fundamental deficiency as the objective of EHR are to provide a holistic view and a complete set of patient's information. (2) Unstable leadership in eHealth Ontario reduced much efficacy in EHR. Employing five Chief Executives in nine years and a 97% reduction of consultant resources in 18 months reduced many of the efficacy and design benefits of the EHR. Some key informants characterized that the EHR program was not built from a functional perspective, but a pressured delivery and a "quickly-built" system that has reduced quality. The experience was that there is a need to demonstrate success to justify the investment.

## 8.6 The Contribution of this Study

This research is a triangulation study that produces strong validation of the collected data, providing findings from a critical realist perspective adding to the understanding of the underlying forces resulting in privacy concerns for patients and healthcare providers. This research also validated and extended the privacy dimension of the CFIP model created in Smith *et al.*, (1996). This research achieved an internal consistency with the Cronbach's alpha value that is stronger than the in Smith, Milberg & Burke's (1996) and Angst & Agarwal (2009), both using the same CFIP model. This study filled a gap in the literature by extending a single stakeholder group to multiple inter-related stakeholder groups surrounding the issues of privacy and efficacy. It explores whether another stakeholder group (providers) have privacy concerns. This research examines the attitudes of three interrelated stakeholders with special attention to exploring countermeasures as a protection mechanism. This research took a social science perspective, which contrasts with the work of Siegenthaler & Birman (2009) to solve privacy protection by engineering and technical procedures. Little has been written in the examination of human elements and attitudes towards sharing private and sensitive personal information, over a distributed communication network in the area of medical health information.

This study has helped to build a foundation and baseline for further evaluation of privacy concerns and efficacy in an EHR system, setting the stage to discuss the what changes are needed to improve the quality and efficacy of this initiative. From a program management perspective, comparison of this study can be made regarding challenges in design, implementation, stable leadership and project governance of the Ontario eHealth organization to other similar organizations implementing EHR in other jurisdictions. It is also recommended to study further the privacy concerns, raised by patients and providers, in this research study. Another future research could be centred on the intricacies that both patients and providers have with privacy concerns in EHR. It is of interest to find out how providers have to calm patient's concerns to encourage more

disclosure of information from patients and at the same time, the provider also practice countermeasures in preventing others from understanding their notes in the EHR and steps should be taken to allow for greater transparency . Future studies could focus on the requirement of providers to enhance the quality of treatment to the patient and the role of increased information sharing and transparency in achieving this.

## **8.7 Limitations of This Research**

This research examines a complex and evolving implementation of the EHR in Ontario, Canada. While the findings provide a lasting understanding of the issues, specific details changed over time. This study expanded on a previous research study of one group to three group of stakeholders. While the internal and convergence validity is strong, a comparison to other jurisdictions would be valuable.

This study has not explored further action and impacts in patients and providers' countermeasures to the sharing of EHR information. All research data from the patient survey, focus group discussion and key informant interviews suggested attitudes, opinions, and insight are time sensitive as their meaning will change over time. A longitudinal study repeated annually or biannually could be useful comparing results against changes occurring in EHR system. Data in this study would not be extrapolated. However, it is plausible to predict that if privacy and confidentiality safeguards are not implemented that both patients and providers will continue to use countermeasures to avoid sharing information across a distributed network. This study is of an exploratory nature and does not constitute any causal relationship. There is potential for the samples collected in the survey, focus group and key informant interviews to be biased as data is captured at a point in time and is a sample study although statistically robust. When new sub-systems of the EHR are introduced, and patients and service

providers are better informed, there is the likelihood that opinions and attitudes will change.

## **8.8 Future Research and High-Level guidelines**

Further research extending from this study could include examining how patients can be persuaded to reduce privacy concerns through better communications and education about how the EHR system works. Angst & Agarwal (2009) study had shown that when providers exercised clear communication and talked with a pleasant tone of voice, patients changed their willingness to provide information in EHR. This future study can build upon and extend the examination of such result using Angst & Agarwal research as a foundation paper. A critical realist approach could be a way to understand how patients perceive truth and reality of their concerns and why they will be opening up to the willingness of change.

Another study could be on the impact of countermeasures exercised by patients and providers. Starting with the concept of countermeasures as risk-mitigation techniques, then a study of how a subject group becomes aware of the privacy concerns from their observation of the frequent breaches of privacy event, and to assesses and establish the perception of risks and eventually forming the perceived “true believe”. Such perceived privacy risks are threats that need to be subsided using countermeasure. The study can then explore the relationship of how such countermeasure results to impacts and effectiveness. The results of both suggested future research can be relayed back to the research findings in this study if similar triangulation technique is used.

## 8.9 Conclusion

Patients have genuine privacy concerns regarding sharing sensitive information in an EHR. Service providers have similar privacy concerns. Both groups have used countermeasure to address these concerns and avoid providing complete information. Such countermeasures reduce the efficacy of EHR. Ontario patients exhibited similar countermeasures as those in the USA such as withholding of information, doctor-hopping and paying out of pocket expenses to avoid information aggregation. The top-down structure of EHR design and implementation used by Canadian Health Infoway (CHI) followed suit some of the significant problems encountered by other EHR initiatives with similar structures. If the Ontario payers had meticulously studied and learned from the experience of others, such as the EHR project from National Health Service in the UK, then perhaps, some of the mistakes in Ontario EHR program could have been avoided.

## 8.10 Reflection

There were several challenges in completing this study. Some were overcome and provided success stories while others eventually become intrinsic limitations to the findings or a lesson learned. Some were by design while others were unforeseen.

### *(1) The EHR program under study is a complex and moving target*

By its nature, this timely and complex EHR initiative is both messy and in an ever-changing environment. It is messy because of the intricacy of the contradicting needs of the three stakeholder groups (the 3Ps). It is a moving target as the collapse of the implementing organization (Smart Systems for Health Agency) was replaced by eHealth Ontario, and that had five changes of leadership (CEOs) in nine years and almost entirely eliminated the consultant resources available in eighteen months. I explored these issues with a bottom-up approach with a survey of patients first. These findings helped establish an

understanding of their privacy concerns and that a sizeable minority were willing to use countermeasures to safeguard their privacy.

I realized that to make sense of this research in this chaotic and continuously changing EHR project I needed to employ triangulation methodology to give meaning, validity, and relevance to the findings. The downside of this triangulation approach is that much data was required and that the recruitments process of the service providers and payers proved to be difficult.

## *(2) Difficulties in the recruitment of the 3Ps*

**Patients** ---To cover the geographical area of the Greater Toronto Area, I used three channels (Street, Online, and Classroom) to survey the patients. I recruited 513 patients. Two concerns emerged: unusable responses and insufficient diversity of the sample. Of the total of 513 forms completed, only 453 (88.3%) were usable. Two problems happened on the street recruitment of patients. First, I recruited patients at an exit of a subway station relying on heavy traffic of potential patients. It proved to be very ineffective as most people were busy hurrying to their destination. A switch to a quieter location, a few streets away yielded the opposite phenomena of too few people and that they were mostly retirees resulting that I was not recruiting participants that are sufficiently diverse in the sample. Finally, I stood on a busy street in the shopping district in downtown Toronto city; many people were walking by and from all walks of life. The second problem is that in a big metropolis, like Toronto, many people avoid contacts from canvassers. I quickly learned that my first greeting with anyone would be “I am not selling anything, I am conducting an academic survey.” I also placed a big poster (Figure 8.1) behind me with an incentive of a draw of a gift card after a completed survey. This arrangement worked well as I had participants whose occupations included judges, lawyers, financial investors, insurance agents, students, and home-makers. Participants were aged between age 18 to 72. One nurse came to me and said that: “I am using EHR every day and I would like to participate in your survey.”



Figure 8.1: Photo on the poster used for enrollment of the patient in Street survey

**Providers** --- Providers, are busy people. I sent emails, followed by letters and sometimes delivered invitations to doctors' offices by hand. There were minimal responses. Providers also work on different schedules so to enroll them in the same room for a focus group discussion was difficult. After three months of unsuccessful enrollment, I finally decided to use a professional services company with expertise in research enrollment for focus groups. This company has expertise in telephone etiquette and also has time to make and receive phone calls from doctors. They were also used in making schedule arrangement for the willing participants to come on a commonly available schedule. I also found that using an external company allows me to prepare a better moderator's script as the guide for the two focus groups.

**Payers** --- One of the payer organization, was skeptical about the objective of the research especially the intended use of the report. They were concerned that the research was intended for exposing their organizational weakness and would scrutinize their operations, expenditure, and funding. It took me three months with many emails and documents to get their participation. In solving this trust problem, my solution was to be very patient, polite and provide detailed

documentation about our research objectives and assure the organization that it is an academic study for scientific knowledge.

*(3): A Large amount of data to process*

For the patient's survey, there are a total of 11,325 data points. Using factor analysis and determining the weighted value of each variable as part of the CFIP was a significant challenge. To determine the primary weighting, I used the Akaike Information Criterion (AIC) and subsequently used the Principal Component Analysis (PCA). However, neither methods provided a good fit to explain the weighting. To ensure that I can explain each step of the calculation and analysis, I eventually used a simple tool, an Excel spreadsheet. I can formulate each formula, each equation, group-count and enumerated each data point to support the result and findings.

*(4) Modified Delphi techniques with doctor group*

Two issues emerged from using Delphi techniques with service providers who are busy medical professionals. The traditional Delphi technique with consensus proposed and sent back to participants by paper report or email, after the meeting, will not work with them. Therefore, a modified instant Delphi technique was used. The discussion was summarized, and participants' verbal agreement or body gesture such as nodding their head to agree with the statements, was noted. The doctor's group has a diversity of opinions and a firm perception of their choices. Sometimes, it is difficult to obtain a complete consensus of the doctor's group, a further modified of the Delphi technique was used with majority opinion become consensus especially when some other doctors had no opinion.

### **8.10.1 Lesson Learned**

Throughout the execution of this research study, the approach in carrying out the tasks, described in the research proposal, needed to be somewhat flexible as long as the result of the objective is met using a sound research method. For instance, I learned that changing research locations in the street survey solved the enrollment problem. Project management and frequent review of task



progress against schedule help initiate alternative approaches. After spending three months contacting over 100 doctors (out of a list of 500 plus), with the intention to form a five-member focus group was unsuccessful. I recognized the needs and exercised the option of using an external professional to help with recruitment.

The building of trust and rapport requires a lot of patience, politeness, and clarity in addressing the needs of the patients, providers, and payers. I have learned that human interrelations in research projects can be executed more efficiently and effectively if I approach the participants with an understanding of their needs. An example was a minus ten-degree Celsius temperature during the street survey, I have invited participants to move into a building with a much warmer temperature to conduct the survey. This allowed for a high quality of interactions and participants did not have to rush through the survey because of coldness. I learned that it is these small, but considerate actions on my part help improved the quality and efficiency of obtaining the research data.

### **8.10.2 Final Words on Reflection**

This section discussed some of the biggest challenges encountered during this research study. While some challenges are by design to increase the quality of the research findings, other problems are unexpected. I have reflected what works and what does not work. One thing I always remember is the insistence of discipline and the uncompromising work process for a scientific study. This reflections and lesson learned have helped me to improve my research skills and would be invaluable in my future research study.

## References

- Alvarez R. (2008). The Canada Health Infoway Plan , Canada Health Infoway powerpoint, p.17
- Alvarez, R (2002). *The promise of e-Health – a Canadian perspective* eHealth International, Ottawa, 2002
- Angst, C. & Agarwal, R. (2009). “Adoption of electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood model and Individual Persuasion”. *MIS Quarterly*, Vol. 33 No. 2, pp. 339-370.
- Apkon, M. & Singhaviranon, P. (2001). Impact of an electronic information system on physician workflow and data collection in the intensive care unit. *Intensive Care Medicine*, (27) 1 pp122-130.
- Arnold S, (2007). Electronic Health Records: A Global Perspective. Health Information and Management Systems Society (HIMSS).
- Ash, J. (2004). "Factors and Forces Affecting EHR System Adoption: Report of a 2004 ACMI Discussion", *Journal of the American Medical Informatics Association*, 12(1), pp. 8-12.
- Bargh, J. A., Chen, M., & Burrows, L. (1996). Automaticity of social behavior: Direct effects of trait construct and stereotype activation on action. *Journal of Personality and Social Psychology*, 71, 230—244.
- Barsauskas, P., Sarapovas, S., & Cvilikas, K. (2008). “The evaluation of e-commerce impact on business efficiency”. *Baltic Journal of Management*, 3 (1), pp. 71-91.
- BBC News (2013). NHS Surrey fined £200,000 after losing patients' records,BBC News July 2013, Available at:  
<http://www.bbc.co.uk/news/technology-23286231> (Accessed: Sep 2013)
- Bernecker, S., & Dretske, F., (2007). *Knowledge: reading in contemporary epistemology*. New York: Oxford University Press.
- Bhaskar, R. (1989). *Reclaiming Reality: A Critical Introduction to Contemporary Philosophy*, Verso, London.
- BioSpace. (2018). *Gamma-Dynacare Medical Laboratories Announces Rebranding to Dynacare BioSpace*. Available at:  
<http://www.biospace.com/News/gamma-dynacare-medical-laboratories-announces/374801> [Accessed 15 Feb. 2017].
- Brown. R, (2006). *Doing Your Dissertation in Business and Management: The Reality of Research and Writing* Sage Publications 2006
- Bryman, A., Bell. B. (2007) “Business Research Methods” Oxford University Press 2 Ed. (2007)
- California HealthCare Foundation. (1999). *National Survey: Confidentiality of Medical Records*. Oakland: CHCF.

Cambridge Dictionary, (2017a). Meaning of “privacy” in the English Dictionary, Cambridge Dictionary, Cambridge University Press, 2017 Available at: <http://dictionary.cambridge.org/dictionary/english/privacy> (Accessed 15 Feb., 2017).

Cambridge Dictionary, (2017b). Meaning of “countermeasures” in the English Dictionary, Cambridge Dictionary, Cambridge University Press, 2017 Available at: <http://dictionary.cambridge.org/dictionary/english/countermeasure> (Accessed 15 Feb., 2017).

Canada Health Infoway. (2004). Electronic Health Record (EHR) Standards Needs Analysis. Ottawa: Canada Health Infoway.

Canada Health Infoway. (2005). "Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture". Canada Health Infoway.

Canada Health Infoway. (2006). “EHRS Blueprint: an interoperable EHR framework.” Canada Health Infoway.

Canadian Institute for Health Information. (2009). “Healthcare in Canada: A decade in review”. Canadian Institute of Health Infomatics.

Carifio, J. & Perla, R. (2007). Ten Common Misunderstanding, Misconceptions, Persistent Myths and Urban Legends about Likert Scales and Likert Response Formats and their Antidotes. *Journal of Social Sciences* 3 (3):106-116, 2007

Cavoukian, A (2004). *A guide to the Personal Health Information Act*, Information and Privacy Commissioner/Ontario Toronto.

Cavoukian, A. (2010). Encrypt Your Mobile Devices: Do It Now. PHIPA Order HO-007 Office of the Information & Privacy Commissioner, Jan 2010

CBC News, (2009) *EHealth scandal a \$1B waste: auditor* CBC News Oct 2009 Available at: <http://www.cbc.ca/news/canada/toronto/ehealth-scandal-a-1b-waste-auditor-1.808640> (Accessed 12 April, 2013)

CBC News. (2009). “Head of eHealth Ontario is fired amid contracts scandal, gets big package”, <http://www.cbc.ca/news/canada/story/2009/06/07/ehealth-kramer.html> (Accessed 12 Dec. 2012) Retrieved on Dec 2012.

CBC News. (2010). “Health costs push Alberta deficit to \$4.7B” CBC News Feb 2010 Available at: <http://www.cbc.ca/news/canada/edmonton/story/2010/02/09/edmonton-alberta-budget-2010.html> (Accessed on April 2012)

CBC News, (2015). ‘Ontario falls short of goal to digitize all health records by end of 2015’ 28 Dec Available at: <http://www.cbc.ca/news/canada/toronto/ehealth-records-1.3380630> (Accessed: Jan 15, 2016)

Charles, D. Gabriel, M. and Searcy, T. (2015). Adoption of Electronic Health Record Systems among U.S. Non- Federal Acute Care Hospitals: 2008-2014, The Office of the National Coordinator for Health Information Technology, ONC Data Brief No. 23 Apr. 2015

- Chartrand, T. L.; Bargh, J.A. (1999). 'The chameleon effect: The perception–behavior link and social interaction. *Journal of Personality and Social Psychology*, Vol. 76(6), Jun 1999, 893-910.
- Chhanabhai, P. N. (2007). Fear of Breach? The New Zealand public's opinion. New Zealand: University of Otago.
- Coiera, E. (2009). Building a National Health IT System from the Middle Out *Journal of the American Medical Informatics Association* Vol. 16 No. 3 pp 271 – 273 Jun 2009
- CONO.(2009). Confidentiality and Privacy, Personal Health Information. Ontario: College of Nurses of Ontario 2009.
- CPSBC, (2014). Professional Standards and Guidelines – Medical Records, College of Physicians and Surgeons of British Columbia, Sept 2014
- CPSO (2006) Confidentiality of Personal Health Information #8-05, College of Physicians and Surgeons of Ontario, Toronto, 2006
- CPSO, (2012 #1). *Mandatory and permissive Reporting* #6 -12, College of Physicians and Surgeons of Ontario, Toronto, 2012
- CPSO, (2012 #2 ). Medical Records Policy statement #4 -12, College of Physicians and Surgeons of Ontario, Toronto, 2012
- CNO, (2009). Confidentiality and Privacy – Personal Health Information, College of Nurses of Ontario, Pub. No. 41069, 2009 Toronto, Ontario
- Craig, E., (2002). Routledge Encyclopedia of Philosophy. General Ed. London: Routledge Manson.
- Crean, K. (2010). Accelerating Innovation In Information And Communication Technology For Health. *Health Affairs*, 29(2), 278-83. Government of Ausatralia. (2010). *HealthConnect*.
- Creswell, J. & Miller, D. (2000). Determining Validity in Qualitative Inquiry *Theory into Practice*, Vol. 39 No. 3, pp.124-130
- Creswell, J. W., Plano Clark, V. L., Gutmann, M., & Hanson, W. (2003). Advanced mixed methods research designs. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioral research* (pp. 209–240). Thousand Oaks, CA: Sage.
- Creswell, J. (2005). Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research, 2<sup>nd</sup> Ed. Pearson Education Inc. New Jersey
- D'Arcy, J. and Hovav, A. (2007). Deterring Internal Information Systems Misuse, *Communication of the ACM*, Oct 2007 Vol 50 no. 10 pp. 113-117
- Davis, C., Stoots, M. (2012). A Guide to EHR Adoption: Implementation Through Organizational Transformation. HIMSS

- Dembe *et al*, (2011). “Statistical software applications used in health services research: analysis of published studies in the U.S”, *BMC Health Services Research* 2011, 11:252.
- Denzin, N. (2006). *Sociological Methods: A Sourcebook*. Aldine Transaction. ISBN 978-0-202-30840-1. (5th edition).
- De Vanujany, F.-X. (2005). Information Technology Conceptualization: Respective Contributions of Sociology and Information Systems. *Information Technology Conceptualization: Respective Contributions of Sociology and Information Systems* 5(1):39-58.
- Doupi P, R. E. (2010). eHealth Strategies, Country brief: Norway. Bonn: European Commission, DG Information Society and Media.
- Dynacare, (2018). Dynacare - Gamma-Dynacare Medical Laboratories Announces Rebranding to Dynacare Available at: <https://www.dynacare.ca/news/gamma-dynacare-medical-laboratories-announces-rebr.aspx> (Accessed: 15 Mar, 2018).
- Eason, K., Dent, M., Waterson, P., Tutt, D. & Thronett, A. (2012). Bottom-up and middle-out approaches to electronic patient information systems: a focus on healthcare pathways, *Informatics in Primary Care*, 2012;20:51-6. British Computer Society. UK
- eCHN (2016) Electronic Child Health Network, home page Available: [www.echn.ca](http://www.echn.ca) (Accessed: Jun 2016)
- eHealth Ontario (2014). Ontario’s Ehealth Blueprint: In-depth, eHealth Ontario, 2014 Toronto, Ontario , Healthcare Information and Management Systems Society (HMISS), Chicago, USA
- eHealth Ontario (2015). ‘EHRs: It’s working for you’ Available at: <http://www.ehealthontario.on.ca/en/progress-report> (Accessed: Jan 15, 2016)
- Ekos report. (2007). Electronic Health Information and Privacy Survey: What Canadians Think — 2007 EKOS Research Associates.
- Fantl, Jeremy, (2016). "Knowledge How", *The Stanford Encyclopedia of Philosophy* (Spring 2016 Edition), Edward N. Zalta (ed.), Available at: <http://plato.stanford.edu/archives/spr2016/entries/knowledge-how/> (Accessed 12 April, 2016)
- Feingold, J. (2011). “Are More Doctors Adopting EHR?” <http://www.nuesoft.com/blog/are-more-doctors-adopting-ehrs/> Retrieved on April 2012.
- Fern, E. (2001). “Advanced Focus Group Research” . California, USA Sage Publications Inc
- Fernández-Alemán, J.; Señor, I.; Lozoya, P. and Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review *Journal of Biomedical Informatics* Vol. 46 (2013) pp. 541–562

- Flaherty, D., (1991). On the Utility of Constitutional Rights to Privacy and Data Protection, *Case Western Reserve Law Review* Vol. 41 Issue 3 pp. 831
- Fortin, P. (2006). "The Baby Boomers' Tab." CBC News. Available at: <http://www.cbc.ca/news/background/canada2020/essay-fortin.html> (Accessed 25 Mar, 2018).
- Fried, C. (1968). "Privacy." *The Yale Law Journal* Vol. 77, No. 3 (Jan. 1968), pp. 475-493
- Frelick, K (2006). Consent\_and\_PHIPA 2004 - Creating the right balance First Annual Privacy Law Summit. Ontario: Ontario Bar Association.
- Frost, J., Vermeulen, I., Beekers, N.(2014). "Anonymity Versus Privacy: Selective Information Sharing in Online Cancer Communities" *Journal of Medical Internet research* 2014 May; 16(5): e126.
- Furnell, S.; Gennatou, P. and Dowland. (2002). "A Prototype tool for Information Security Awareness and Training", *Logistics Information Management*, Vol. 15 Iss 5/6 pp. 352 – 357
- Gagnon, M., Shaw, N., Sicotte, C., Mathieu L., Leduc, Y., Duplantie, J., Maclean, J. and Leare, F. (2019). Users' perspectives of barriers and facilitators to implementing EHR in Canada: A study protocol, BioMed Central Ltd. Available at: <https://implementationscience.biomedcentral.com/articles/10.1186/1748-5908-4-20> (Accessed 15 Mar. 2017).
- Garson. D. (2016) Validity & Reliability, Statistical Association Blue Book Series 2016
- Gemma, W., (2014). The 6 Types Of Knowledge: From A Priori To Procedure May 19, 2014 Available at: <https://blog.udemy.com/types-of-knowledge/>
- Goldstein *et. Al.*, (2006) "Patient Safety in Guideline-Based Decision Support for Hypertension Management: ATHENA DSS" *Journal of the American Medical Informatics Association*, Volume 9, Issue Supplement\_6, 1 November 2002, Pages S11–S16
- Griener, G. (2005). Electronic Health Records as a Threat to Privacy, *Health Law Review University of Alberta*, Volume 14, Number 1 pp 14 – 15
- Grudens-Schuck, N., Allen, B. L., & Larson, K. (2004, May). Focus group fundamentals. Ames, IA: Iowa State University Extension. Available at <http://www.extension.iastate.edu/Publications/PM1969B.pdf>. (Accessed Mar 2, 2018)
- Hammond, E. (2002). "What if we really had an electronic health record?". *EuroRec2002*. Berlin: EuroRec 2002.
- Hayrinen, K., Saranto, K., & Nykanen, P. (2008). Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International journal of medical informatics*, (77) 291–304.

Harman, L.; Flite, A., & Bond, K., (2012). Electronic Health Records: Privacy, Confidentiality, and Security, American Medical Association Journal of Ethics, Vol. 4, No. 9 pp.712-719

Heale, R. & Twycross, A. (2015). "Validity and Reliability in Quantitative Studies. Evidence Based Nursing", Vol, 18 No. 3 pp. 66-67 May, 2015

Health Care in Canada. (2009). "A Decade in Review" Available at: [http://secure.cihi.ca/cihiweb/products/HCIC\\_2009\\_web\\_e\\_Ch3.pdf](http://secure.cihi.ca/cihiweb/products/HCIC_2009_web_e_Ch3.pdf) (Accessed on Dec 2012).

Health & Medicine. (2006). "At risk of exposure: In the push for electronic medical records, concern is growing about how well privacy can be safeguarded". Los Angeles Times.

Health Governance Report. (2007). Protect patient privacy when going electronic to reduce risk. Health Governance Report.

Henriksen, E.; Burkow, T.; Johnsen, E. and Vognild, L. (2013). Privacy and Information Security Risks in a Technology Platform for Home-Based Chronic Disease Rehabilitation and Education *BMC Medical Informatics and Decision Making* 2013, 13:85

Herrmann, D. (2007). Complete Guide to Security and Privacy Metrics: Measuring Regulatory: Measuring Regulatory Compliance, Operational Resilience, and ROI CRC Press 2007 Fl

HIMSS, (2011). Health Information and Management Systems Society. EHR: electronic health record. Available at: [http://www.himss.org/ASP/topics\\_ehr.asp](http://www.himss.org/ASP/topics_ehr.asp). (Accessed January 25, 2011)

Hodge, T. (2011). EMR, EHR, and PHR – Why All the Confusion? Canada Health Infoway, Available at: <https://www.infoway-inforoute.ca/en/what-we-do/blog/digital-health-records/6852-emr-ehr-and-phr-why-all-the-confusion> (Accessed 18 Feb. 2017).

Hoyt, R.; Yoshihashi, A. (2014). *Health Informatics: Practical Guide for Healthcare and Information Technology Professionals*. 6<sup>th</sup> ed. Lulu. com.

IPC, (2005a). Photograph of patient in newspaper article Office of the Information & Privacy Commissioner/Ontario HC-050002-1 Apr 2005

IPC, (2005b). Patient's Concerns About Fundraising Resolved Office of the Information & Privacy Commissioner/Ontario HC-50001-1 Sep 2005

IPC, (2005c). Order HO-001 Office of the Information & Privacy Commissioner/Ontario Oct 2005

IPC, (2005d). Patient requesting correction to information contained in her health record Office of the Information & Privacy Commissioner/Ontario Oct 2005

Ipsos Reid. (2012). What Canadian Think: Electronic Health Information Survey 2012 Canada Health Infoway.

- Irwin, K. (2014). Patient Deception of Doctors Market Research Associate, Software Advice Available at: <http://www.softwareadvice.com/medical/industryview/patient-deception-report-2014/> (Accessed 26 May, 2016)
- ISO TIC20514. (2004). ISO TIC 215 Health informatics — Electronic health record — Definition, scope, and context. International Standard Organization. International Standard Organization
- Jacobson, P. (2002). Symposium: Modern studies in privacy law: National Health Information Privacy regulations under. Minnesota Law Review, 86.
- Johnston, Douglas, *et al.* (2003). "The Value of Computerize Provider Order Entry in Ambulatory Settings: Executive Preview." Wellesley, MA: Center for Information Technology Leadership 2003".
- Jorge Larrain (1979). The Concept of Ideology p.197, Available at: <http://www.autodidactproject.org/other/ideo10.html> (Accessed 1 March, 2016)
- Kapushion, M. (2004). "Hungry, hungry HIPAA: When privacy regulations go too far". Fordham Urban Law Journal, 31.
- Krueger, R. & Casey, M (2000). Focus groups: A Practical Guide for Applied Research.
- La Forest *et al.*, (1992). McInerney v, MacDonald, Supreme Court Judgement, Case number: 21899, Report: [1992] 2 SCR 138. Available at: <http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/884/index.do> (Accessed 10 Oct, 2014)
- Lake Research Partners and the American Viewpoint. (2006). National Survey on Electronic Personal Health Records, Survey Finds Americans Want Electronic Personal Health Information to Improve Own HealthCare. Lake Research Partners and the American Viewpoint.
- Larsen, K., Allen, G., Vance, A., Eargle, D. (2015). Theories Used in IS Research Wiki. Retrieved Jan 2015 Available at: <http://IS.Theorizeit.org>.
- Leonidas et al (2012). *Challenges in implementing nationwide electronic health records: lessons learned and how should be implemented in Greece* 10<sup>th</sup> International Conference on Information Communication Technologies in Health, July 2012 Samos Island Greece
- Levy, Y. and Ellis, T. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research *Informing Science Journal* Vol. 9 pp.181-212 2006
- Likert, R. & Hayes, S. (1957). Some Applications of Behavioural Research. Paris, Unesco.
- Macionis, J.; Gerber, L. (2010) Sociology, Seventh Canadian Ed., Pearson Canada (2010)
- Maughan, A. (2010). *Six reasons why the NHS National Programme for IT failed* ComputerWeekly.com TechTarget, London Sep 2010



MBSW, (2006). *Epistemology Study Guide*, Manchester Business School Worldwide, (s.l.) Manchester, UK

McCarter, J. (2009). Ontario's Electronic Health Records Initiative, Office of the Auditor General of Ontario,

McCarthy, K. (2014). Study: 50 Percent of Patients withhold information from their Doctor NueMD, 2014] Available at:  
<http://www.nuemd.com/news/2014/12/19/study-50-percent-patients-withhold-information-their-doctor> (Accessed 12 May, 2015)

McClanahan, K. (2008). Balancing Good Intentions: Protecting the Privacy of Electronic Health Information. *Bulletin of Science Technology Society*, pp. 69-74.

McDowell, I. (2006). *Measuring Health: A guide to Rating Scales and Questionnaires*, 3<sup>rd</sup> Ed. Oxford University Press, New York

McGinn, C., Grenier, S., Duplantie, J., Shaw, N., Sicotte, C., Mathieu, L., Leduc, Y. Legarie, F. & Gagnon M. (2011). Comparison of User Groups' Perspective of Barriers and Facilitators to Implementing Electronic Health Records: A systematic Review, *Biomed Central* Available at:  
<http://www.biomedcentral.com/1741-7015/9/46> (Accessed 6 April, 2014)

McLeod, P. (2013). 'Future of electronic health records agency in question', *Herald News*, 19 Apr . Available at:  
<http://thechronicleherald.ca/canada/1124012-future-of-electronic-health-records-agency-in-question> (Accessed: Jun 13 2016)

Menachemi, N, Brooks, R. (2006). "Reviewing the Benefits and Costs of Electronic Health Records and Associated Patient Safety Technologies" *Journal of Medical Systems*, June 2006, Volume 30, Issue 3, pp 159-168

Merriam-Webster. Dictionary, (2017). Definition of Privacy. Merriam-Webster 2017 Available at: <https://www.merriam-webster.com/dictionary/privacy> (Accessed 15 Feb. 2017).

Microsoft (2014) Support for Windows XP ended, Available at:  
<https://www.microsoft.com/en-us/windowsforbusiness/end-of-xp-support> (Accessed Oct 2017)

Minister of Justice (2017). Personal Information Protection and Electronic Documents Act, Minister of Justice (2017)

Ministry of Social Affairs and Health. (2002). National Definition and Implementation of the Electronic Patient Record System. Ministry of Social Affairs and Health, National Health Services UK. (2010).

MOH, (2004). *Personal Health Information Protection Act, 2004: An Overview* , Ministry of Health and Long Term Care Available at:  
[http://www.health.gov.on.ca/en/common/legislation/priv\\_legislation/personal\\_info.aspx](http://www.health.gov.on.ca/en/common/legislation/priv_legislation/personal_info.aspx) (Accessed 12 April, 2016)

- Morrison et al, (2010). *Understanding Contrasting Approaches to Nationwide Implementations of Electronic Health Record Systems: England, the USA and Australia* Journal of Healthcare Engineering Vol 2 No. 1 2011 pp 25-41
- Morse, J. M. (1991). Approaches to qualitative-quantitative methodological triangulation. *Nursing Research*, 40, 120–123.
- Morton, M., Wiedenbeck. S (2009). A Framework for Predicting EHR Adoption Attitude - A Physician survey.pdf. p.6.
- NAPRA (2009A). National Association of Pharmacy Regulatory Authorities. Supplemental Standards of Practice for Schedule II and III Drugs. June 2005. [http://www.napra.ca/pages/Practice\\_Resources/supplemental\\_standards\\_of\\_practice\\_for\\_schedule\\_II\\_and\\_III\\_drugs.aspx](http://www.napra.ca/pages/Practice_Resources/supplemental_standards_of_practice_for_schedule_II_and_III_drugs.aspx)
- NAPRA, (2009B). Model Standards of Practice for Canadian Pharmacists, National Association of Pharmacy Regulatory Authorities, March 2009, Ottawa
- New London Consulting, (2011). Canada: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes FairWarning 2011
- Nordgren, A., (2015). Privacy by Design in Personal Health Monitoring *Health Care Analysis* June 2015. Vol. 23, no 2, pp. 148-164
- Nunnally JC (1978). *Psychometric Theory*, 2nd ed., New York, McGraw-Hill Book Company.
- OAG, (2009). Electronic Health Records Report of the Auditor General of Canada to the House of Commons Chapter Four, Office of the Auditor General of Canada
- OCCRP, (2016). Giant Leak of Offshore Financial records Exposes Global Array of Crime and Corruption. The International Consortium of Investigative Journalists 03 April 2016 Available at: <https://www.occrp.org/en/panamapapers/overview/intro/> (Accessed: July 2016)
- Office of Auditor General of Canada (2010). Electronic Health Records in Canada—An Overview of Federal and Provincial Audit Reports 2010 April Report of the Auditor General of Canada. Office of Auditor General of Canada, 2010.
- OMA, (2013). eHealth Policy Paper, Ontario Medical Association Sep 2013
- Ontario, TCOPASO. (2006). Confidentiality of Personal Health Information Policy, Policies & Publication College of Physicians and Surgeons of Ontario. Ontario: The College of Physicians and Surgeons of Ontario.
- Oxford Learner's Dictionary, (2017). Definition of privacy (noun) in English, Oxford Learner's Dictionary, Oxford University Press, 2017 Available at: <http://www.oxfordlearnersdictionaries.com/definition/english/privacy> (Accessed 15 Feb. 2017).

OPC, (2000). *The Personal Information Protection and Electronic Documents Act (PIPEDA)* Office of the Privacy Commissioner of Canada, 2015  
available : [https://www.priv.gc.ca/leg\\_c/leg\\_c\\_p\\_e.asp](https://www.priv.gc.ca/leg_c/leg_c_p_e.asp)

OPC (2011). *PIPEDA and your practice --- A privacy Handbook for Lawyers*  
Office of the Privacy Commissioner of Canada

Orlikowski, W.J., and J.J. Baroudi. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research* 2(1):1-28.

Parker, J. C., & Thorson, E. (2009). Health communication in the new media landscape. In M. Haider, S. C. Ratzan, & W. Meltzer, International innovations in health communication. (pp. 373-394). New York: Springer Publishing Co.

PHAC, (2009). *Formative Evaluation of the Integrated Strategy on Healthy Living and Chronic Diseases* Public Health Agency of Canada 2008-09  
Available at: ([http://www.phac-aspc.gc.ca/about\\_apropos/reports/2008-09/hlcd-vsmc/surveillance/index-eng.php](http://www.phac-aspc.gc.ca/about_apropos/reports/2008-09/hlcd-vsmc/surveillance/index-eng.php)). (Accessed 11 Dec, 2012)

Ravi. (2008). Implementing Electronic Health Records (EHR) Successfully. The healthcare transformation URL:<http://blogs.biproinc.com/healthcare/?p=15> .  
(Accessed 2 Feb. 2013)

Schoen, C., Hayes, S., Collins, S., Lippa, J., & Radley, D. (2014). America's Underinsured: A State-by-State Look at Health Insurance Affordability Prior to the New Coverage Expansions, The Commonwealth Fund 2014

Shaw, A. (2016). Sunnybrook's MyChart PHR Has 140,000 Users in Canada and Abroad *Canadian HealthCare Technology*, Vol. 21, No. 8, Nov 2016 pp. 8

Shellock, F. and Spinazzi, A. (2008). 'MRI Safety Update 2008: Part 1, MRI Contrast Agents and Nephrogenic Systemic Fibrosis' *American Journal of Roentgenology* 2008 191(4), pp. 1129-1139

Siegenthaler, M., Birman, K. (2009). Sharing Private Information Across Distributed Databases, Network Computing and Application(NCA) IEEE

Sinnott, R., Ajayi, O., & Stell, A. (2009). Data Privacy by Design: Digital Infrastructures for Clinical Collaborations. 2009 International Conference on Information Security and Privacy (ISP-09). Orlando: ISP-09.

Smit, M.; McAllister, M. and Slonim, J. (2005). Privacy of Electronic Health Records: Public Opinion and Practicalities. Networking and Electronic Commerce Research Conference (NAEC 2005), Riva Del Garda, Italy, October 2005

Smith, D. & Chua, C (2012). *Business Statistics: A Two-Semester Text*, 9<sup>th</sup> Ed., Prentice Hall, 2012

Smith, J., Milberg, S., & Burke, S. (1996). "Information privacy: measuring individuals' concerns about organizational practices". *MIS Quarterly*. Vol.(20) 2 pp. 167-196

Sparkes, A.W. (1981). The Right to be Let Alone: A Violation of Privacy, *AUSocLegPhilB* 17; (1981) 20 *Bulletin of the Australian Society of Legal Philosophy* 58

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York: New York University Press.

Solove, J. (2008). *Understanding Privacy*. Cambridge, Mass.: Harvard University Press 2008

StatCan (2015). Canada's population estimates: Age and sex, July 1, 2015. *The Daily*, Statistics Canada, Ottawa, Sep 29, 2015

StatCan, (2016). Population of census metropolitan areas Feb 2016, Available at: <http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/demo05a-eng.htm>

Stausberg, J., Koch, D., Ingenerf, J., & Betzler, M. (2003). Comparing paper-based with electronic patient records: lessons learned during a study on diagnosis and procedure codes. *Journal of America Institute for Medical Informatics*, 10 (5) 470-477.

Stead, W. W., Kelly, B. J., & Kolodner, R. M. (2005). Achievable steps toward building a national health information infrastructure in the United States. *Journal of the American Medical Informatics Association* Vol.12 I2, 113-120.

Stewart, K., & Segars, A. (2002). "An Empirical Examination of the Concern for Information Privacy Instrument". *Information Systems Research*, Vol. 13, No. 1, 36-49.

Stroetmann, E. (2011). *European countries on their journey towards national eHealth infrastructures*. Brussels, Belgium: European Commission Information Society.

TAF, (2010). "Find out what any acronym, abbreviation, or initialism stands for" Available at: <http://www.acronymfinder.com/> (retrieved April 6, 2010)

Thakkar, M., & Davis, D.C. (2006). "Risks, Barriers, and Benefits of EHR Systems: A Comparative Study Based on Size of Hospital" *Perspective in Health Information Management*. 2006; 3: 5. Published online 2006 August 14.

Thatcher, R. (2010). Validity and Reliability of Quantitative Electroencephalography (qEEG). *Journal of Neurotherapy*, Vol.14, pp. 122-152

Toronto Star. (2007). Sick Kids doctor loses data on 3,300 patients, *The Star* Available at: [https://www.thestar.com/news/2007/08/31/sick\\_kids\\_doctor\\_loses\\_data\\_on\\_3300\\_patients.html](https://www.thestar.com/news/2007/08/31/sick_kids_doctor_loses_data_on_3300_patients.html) (Accessed May 15, 2014)

Tresopakol, W. (2014). 'Book Review Advanced Focus Group Research' *International Journal of Behavioral Science*, 2014, Vol. 9. Issue 1, 83-86

The government of Ontario (2017). Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31, Government of Ontario e-Laws currency date Mar 22, 2017 Available at: <https://www.ontario.ca/laws/statute/90f31> (Accessed 20 Mar. 2017).

The Telegraph (2012). NHS lost 1.8 million patient records in a year, The Telegraph, Oct 2012 Available at: <http://www.telegraph.co.uk/news/health/news/9640168/NHS-lost-1.8-million-patient-records-in-a-year.html> (Accessed: 11 Mar 2013)

Thomson, J., (1975). The Rights to Privacy, *Philosophy & Public Affairs* Vol. 4, No. 4, pp. 295-314 JSTOR, [/stable/1321160](https://www.jstor.org/stable/1321160)

Tremblay, M.-A. (1957). *The Key Informant Technique: A Nonethnographic Application*. *American Anthropologist*, 59: 688–701.  
doi:10.1525/aa.1957.59.4.02a00100

Wafa. T. (2010). ‘How the Lack of Prescriptive Technical Granularity in HIPAA Has Compromised Patient Privacy’. *Northern Illinois University Law Review* 30 pp3

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 6(1), article 3. Available at <http://dx.doi.org/10.5817/CP2012-1-3> privacy (Accessed Jul 20. 2017)

Wanous, J., Reichers, A., & Hudy, M. (1997). ‘Overall Job Satisfaction: How Good Are Single-Item Measures?’. *Journal of Applied Psychology*, (82:2), pp. 247-252.

Warren, S.& Brandeis, L., (1890). The Right to Privacy, *Harvard Law Review*, Vol.4, No. 5 (Dec 15, 1890), pp. 193-220

Webster, T., (2017). “It’s Really Difficult to Get Your Medical Records in a Usable Format” Available at: <https://tonywebster.com/2015/05/its-really-difficult-to-get-your-medical-records-in-a-usable-format/> (Accessed 15 Mar. 2017).

Wechsler, J. (2006). Medicare, consumerism and IT to shape managed care in 2006. *Managed Healthcare Executive*, 16.

Wikgren M (2004). “Critical realism as a philosophy and social theory in information Science?” *Journal of Documentation*, Vol. 61 No. 1, 2005 pp. 11-22

Wilson, K. (2013). Perception and reality. *New Philosopher*, 1 (2). pp. 104-107

Xu, H.; Rosson, M.; Gupta, S. & Carroll, J. (2002.) Measuring Mobile Users’ Concerns for Information Privacy. The Third International Conference on Information Systems, Orlando, 2012

Xu, H., Dinex, T.; Smith, J. & Hart, P., (2001). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances *Journal of the Association for Information Systems* Vol. 12 Issue 12. Pp. 798-824

Yan, Q., Chang, A. (2007). Threats and Countermeasures for Information System Security: A Cross-Industry Study,” *Information & Management*, Vol. 44, No. 5. pp. 480-491.



## PART 2: Concerns for Information Privacy in Electronic Health Record

Q5	<u>Patient privacy concerns about an EHR</u>	strongly disagree	disagree	neutral	agree	strongly agree	Comments
a.	It usually bothers me when health service providers ask me to provide personal health information.	1	2	3	4	5	
b.	All the personal health information in computer databases should be double-checked for accuracy, regardless of cost.	1	2	3	4	5	
c.	Service providers should not use personal health information for any purpose unless this has been authorized by the individual who provided the information.	1	2	3	4	5	
d.	Service providers should devote the necessary time and effort to prevent unauthorized access to personal information.	1	2	3	4	5	
e.	When service providers ask me for personal health information, I sometimes think twice before providing it.	1	2	3	4	5	
f.	Service providers should take necessary and appropriate steps to make sure that the personal health information in their files is accurate.	1	2	3	4	5	



g.	When patients give personal information to a service provider for a particular reason, the service provider should not use the information for other unrelated reasons (such as for commercial benefits).	1	2	3	4	5	
h.	Service providers should have procedures in place to correct errors in patient's information in a timely manner.	1	2	3	4	5	
i.	Computer databases that contain my personal health information should be protected from unauthorized access, regardless of cost.	1	2	3	4	5	
j.	It bothers me to give a lot of personal information to service providers.	1	2	3	4	5	
k.	Service providers should never sell EHR personal information to other organizations.	1	2	3	4	5	
l.	Service providers should devote the necessary resources, time and effort towards verifying the accuracy of patients' health information in their computer systems.	1	2	3	4	5	
m.	Service providers should not share personal health information with companies unless this has been authorized by the individual who provided the information.	1	2	3	4	5	

n.	Service providers should take necessary steps to ensure that unauthorized people cannot access personal information in their EHR system.	1	2	3	4	5	
o.	I am concerned that service providers are collecting too much personal health information about me.	1	2	3	4	5	
p.	I think that service providers can keep my data secure and private.	1	2	3	4	5	
q.	I am willing to give more health and other private information to the providers if my illness becomes severe.	1	2	3	4	5	

### PART 3: Scenario-Based Multi-criteria Decision

We will start with a scenario. **What would be your answer IF you find yourself in these situations?**

Choose the most severe response that you will take. (1 = least severe, 5 (or 7) is the most severe in terms of restrictions on providing private information)

(A) If your doctor shares your health information with a third party (such as an insurance company or an employer that provides you with benefits or a salary) **WITHOUT** your consent, you would most likely:

- 1- Do nothing
- 2- Express your concern to your doctor
- 3- Ask your doctor to take corrective action to your satisfaction
- 4- Call the third party to tell them they have no rights to use your information
- 5- File a complaint with the Privacy Commissioner and request their assistance
- 6- Seek legal advice
- 7- Sue your doctor for damages caused.

Answer: \_\_\_\_\_

(B) Suppose you have contracted a disease that is normally transmitted sexually. You consider your medical condition private and your family doctor does not know about it. Disclosing your condition will invite a treatment program that might result in you being rejected by your partner and friends. During your regular check-up with your family doctor, you would most likely:

- 1- Give him the full details of this private medical condition, so that he can refer you to a specialist
- 2- Ask him whether it is important for him to know
- 3- Bring up the condition to gather information but do not say that it applies to you, such as saying a friend has this problem
- 4- Tell him part, but not all, of the private information
- 5- Not let your doctor know at all

Answer: \_\_\_\_\_

(C) Suppose you are a professional driver shipping goods between Canadian provinces. A nurse makes you aware of the very high possibility that you are suffering from Obstructive Sleep Apnea (OSA) and you believe the nurse's observation. Such disease could cause you to fall asleep while operating a motor vehicle such as your commercial trailer. Your doctor told you that he is required to report OSA to the ministry of transportation if his patients suffer from it. You know that you could lose your driving privileges and your job as a result. What will you let your doctor know?

- 1- You will give him the full details of your OSA and hope that the disease is treatable
- 2- You will tell him that you might have a mild case of OSA
- 3- You will tell him that you are not sure if you have OSA but you want to find out more information
- 4- You will take precautions against such disease, but do not tell the doctor about your OSA
- 5- You will never tell anyone about the disease regardless of the situation.

Answer: \_\_\_\_\_

(D) Suppose you have a medical condition (disease) that you consider private and that is known only to you. One day, you are being treated in an emergency room for an apparent heart attack. When will you let the emergency doctor who provides services to you know about this medical condition (disease)?

- 1- Let him know right away regardless of your medical condition
- 2- Let him know if you think that by giving him your private medical condition, you will help him to provide better care for you.
- 3- Let him know if you think you are in a life-threatening condition regardless of whether this will be of any use to him
- 4- Don't tell him anything until you find out the severity of your current condition
- 5- Never, even if you are in a life-threatening condition

Answer: \_\_\_\_\_

(E) Suppose you have a medical condition that you want to keep private because disclosure will embarrass you. The doctor assures you that the Electronic Health Record about his patient's private condition will be kept private, but you see that the receptionist in your doctor's office reads patient health records to satisfy her curiosity and pass the time. The receptionist is also a resident of your community and is an active member. Will you tell the doctor about your medical condition that you consider private?

- 1- Yes, but ONLY with the opportunity that the medical receptionist is not on-duty that day
- 2- Yes, but will also make a complaint to the doctor about the wrongdoing of his receptionist
- 3- Yes, but in order to avoid the receptionist, you will go through the trouble of seeing the doctor in another of his clinics even if it is an hour away
- 4- No, do not trust the doctor anymore, as he does not have control over his policy of keeping the EHR private
- 5- No, you will change to another doctor, as there are other doctors available

Answer: \_\_\_\_\_

(F) Suppose you regularly manage information using the Internet, (e.g. pay bills electronically, check banking accounts). If you were allowed to manage the accuracy of your Electronic Health Record, what would you likely do?

- 1- Do nothing. You are not interested in having any access to your Electronic Health Record
- 2- You would login and check that your information is accurate, especially after major medical tests and procedures.
- 3- You would check the accuracy of information and request changes to incorrect information by the service provider
- 4- You would like to have the ability to indicate which information you would like to keep private
- 5- You would like to have a “Privacy Profile” in the system where you can specify what kind of information should be kept private

Answer: \_\_\_\_\_

## Appendix B: List of Academic Search Engines and Resources

Below is a list of academic search engine that was selected and some of them were used as part of the literature review and resources locator for this thesis. In addition to the essential link such as PubMed, MIS Quarterly, many of the above resources links are from “An Internet MiniGuide Annotated Link Compilation by Zillman, Marcus P.”

1. Academic Archive Online – DiVA  
<http://www.diva-portal.se/index.xsql?lang=en>
2. Academic Index <http://www.academicindex.net/>
3. A Collection of Special Search Engines  
<http://www.leidenuniv.nl/ub/biv/specials.htm>
4. All Academic: An Academic Search Engine and Index <http://www.all-academic.com/>
5. Archival Search Engines <http://www.tulane.edu/~lmiller/search.htm>
6. Archives Hub <http://www.archiveshub.ac.uk/>
7. ARL Directory of Scholarly Electronic Journals and Academic Discussion Lists <http://dsej.arl.org/dsej/>
8. ArticleFinder Search - Infotrieve Online  
<http://www4.infotrieve.com/search/databases/newsearch.asp>
9. Article INIST Search INIST Catalog of Articles and Monographs  
<http://services.inist.fr/public/eng/conslt.htm>
10. Australian Journals Online <http://www.nla.gov.au/ajol/>
11. BASE Bielefeld Academic Search Engine  
[http://base.ub.uni-bielefeld.de/index\\_english.html](http://base.ub.uni-bielefeld.de/index_english.html)
12. Behavioral and Brain Sciences (BBS) <http://www.bbsonline.org/>

13. BPubS.com - The Business Publications Search Engine  
<http://www.bpubs.com/>
14. Canadian Association of Research Libraries - Open Archives Metadata Harvester  
<http://carl-abrc-oai.lib.sfu.ca/>
15. CIA FOIA - Electronic Reading Room - Search Options  
[http://www.foia.cia.gov/search\\_options.asp](http://www.foia.cia.gov/search_options.asp)
16. CiteSeer □ Scientific Literature Digital Library  
<http://citeseer.ist.psu.edu/>
17. Clinical Medicine and Health Research Netprints  
<http://clinmed.netprints.org/home.dtl>
18. CS-Structure Academic Search <http://cs-structure.inr.ac.ru/>
19. Directory of Open Access Journals (DOAJ) <http://www.doaj.org/>
20. Distributed Search Engines <http://www.openp2p.com/pub/t/74>
21. DocSource <http://www4.infotrieve.com/search/docsource.asp>
22. DoIS Documents in Informtion Science <http://dois.mimas.ac.uk/>
23. eBizSearch <http://gunther.smeal.psu.edu/>
24. EEVL's Ejournal Search Engines <http://www.eevl.ac.uk/eese/eese-eevl.html>
25. EEVL Xtra <http://www.eevlextra.ac.uk/>
26. Electronic Journal Miner <http://ejournal.coalliance.org/>
27. eScholarship Repository <http://repositories.cdlib.org/escholarship/>
28. Fields of Knowledge <http://www.fieldsofknowledge.com/index.html>

29. GEM <http://www.gemcatcher.com/>
30. Google Scholar Search <https://scholar.google.ca/>
31. Healthcare Resources <http://www.HealthcareResources.info/>
32. Privacy Resources <http://www.PrivacyResources.info/>
33. HighBeam Research <http://www.highbeam.com/>
34. Highly Cited Researchers...<http://isihighlycited.com/>
35. HighWire Press -- Search Multiple Journals  
<http://highwire.stanford.edu/cgi/search/>
36. HONselect Health on the Net Select Search <http://www.hon.ch/MeSH/>
37. Index to University Sponsored Open Access Repositories of Journals  
and Research Materials <http://wiki.dspace.org/DspaceInstances>
38. INFOMINE: Scholarly Internet Resource Collections  
<http://infomine.ucr.edu/>
39. Infotrieve Online <http://www3.infotrieve.com/search/articlefinder.asp>
40. Issue Crawler  
<http://wiki.issuecrawler.net/bin/view/Issuecrawler/WebHome>
41. JSTOR <http://www.jstor.org/>
42. Life Science Journals Archives <http://www.pubmedcentral.gov/>
43. myLITsearch Scholarly Resources for Academic Research  
<http://www.mylitsearch.org/>
44. New England Journal of Medicine  
<http://www.nejm.org/doi/pdf/10.1056/NEJMp058128>
45. NELLCO Legal Scholarship Repository <http://lsr.nellco.org/>



46. NewJour <http://gort.ucsd.edu/newjour/search.html>
47. Oxford Scholarship Online  
<http://www.oxfordscholarship.com/oso/public/index.html>
48. Public Library of Science <http://www.publiclibraryofscience.org/>
49. Pubmeds government <https://www.ncbi.nlm.nih.gov/pubmed/>
50. PubMed Central <http://pubmedcentral.com/>
51. Registry of U.S. Government Publication Digitization Projects  
<http://www.gpoaccess.gov/legacy/registry/>
52. SciELO - Scientific electronic library online  
[http://www.scielo.cl/scielo.php?script=sci\\_home&lng=en&nrm=iso](http://www.scielo.cl/scielo.php?script=sci_home&lng=en&nrm=iso)
53. Science Research <http://www.ScienceResearch.com/>
54. Search Engines Colossus Academic Search Engines  
<http://www.searchenginecolossus.com/Academic.html>
55. Serials in Cyberspace Collections, Resources and Services  
<http://www.uvm.edu/~bmaclenn/>
56. Social Informatics <http://www.SocialInformatics.info/>
57. TechXtra - Indepth Academic and Scholar Search  
<http://www.techextra.ac.uk/>

\*\*\*\*\*