

**AN EXPLORATORY STUDY OF REGISTERED NURSES' EXPERIENCES IN
PATIENT INFORMATION PRIVACY AND SECURITY WITHIN THE PROVINCES
OF ALBERTA (AB) AND SASKATCHEWAN (SK)**

A Thesis Submitted to the
College of Graduate and Postdoctoral Studies
In Partial Fulfillment of the Requirements
For the Degree of Doctor of Philosophy
In the Department of Interdisciplinary Studies
University of Saskatchewan
Saskatoon

By

EBENEZER SACKEY, BSc., MSc., MISSM., MBA, PhD

© Copyright Ebenezer Sackey, March, 2021. All rights reserved
Unless otherwise noted, copyright of the material in this thesis belongs to the author

MEMBERS OF ADVISORY COMMITTEE

PhD Candidate:

Ebenezer Sackey MISSM, M.Sc., MBA, InterD PhD,
Interdisciplinary Studies,
University of SK.
Email: ebenezer.sackey@rdc.ab.ca

Research Supervisor

Arlene Kent-Wilkinson RN, CPMHN(C), BSN, MN, PhD,
Associate Professor, College of Nursing, University of SK.
Email: arlene.kent@usask.ca

Committee Member

Keith A. Willoughby, B. Comm., MSc, Ph.D,
Professor of Management Science
Dean, Edwards School of Business,
University of SK.
Email: willoughby@edwards.usask.ca

Committee Member

David Burgess UE, BA(Hons), LetA(Hons), BEd(Dist), MEd, PhD,
Associate Professor,
Department of Educational Administration, University of SK.
Email: david.burgess@usask.ca

Committee Member

Sandra Bassendowski RN, B.Ed., M.Ed., EdD,
Professor Emeritus, College of Nursing,
Regina Campus, University of SK.
Email: s.bassendowski@usask.ca

Committee Chair

Linda Ferguson RN PhD Pro.Dir©
Professor Emeritus, College of Nursing, University of SK.
Email: linda.ferguson@usask.ca

Committee Member (d. 2018, in memory of)

Jim Greer B.Sc., B.Ed., M.Ed., M.Sc., Ph.D,
Professor of Computer Science and Senior Strategist, Learning Analytics,
University of SK.

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a doctor of philosophy degree from the University of SK, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by Dr. Arlene Kent-Wilkinson who supervised my thesis work or, in her absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of SK in any scholarly use which may be made of any material in my thesis.

Requests for permission to copy or to make other uses of materials in this thesis/dissertation in whole or part should be addressed to:

Chair, Interdisciplinary Studies Program
College of Graduate and Postdoctoral Studies
University of SK
116 Thorvaldson Building, 110 Science Place
Saskatoon, SK S7N 5AC9, Canada

OR

Dean, College of Graduate and Postdoctoral Studies
University of SK
116 Thorvaldson Building, 110 Science Place
Saskatoon, SK S7N 5C9
Canada

ABSTRACT

The purpose of this qualitative research was to gain a better understanding of the experiences of registered nurses in patient information privacy and security in Alberta (AB) and Saskatchewan (SK) health regions. Studies of this nature are rarely if ever conducted as topics like ethics, breaches, and self-reflection of our own professional practices are sensitive in nature to all health care professionals. Exploring patient information security/privacy falls into this delicate and complex category. As an outsider to the nursing profession/discipline, I had the privilege of conducting this study. Surprisingly, twenty nurses from the medical/surgical/critical care specialties did agree to participate in this study. Interpretive Description (ID) was the methodology chosen for this study. Face to face interviews were conducted with twelve nurses from large and small cities in each of two neighboring Prairie provinces in Canada. Nine nurses from AB and eleven nurses from SK shared their experiences of compliance to their regulatory health information Acts in each province: The Alberta *Health Information Act* (HIA), and the Saskatchewan *Health Information Protection Act* (HIPA). Unexpectedly, new definitions of what constitutes patient information privacy and security, and what comprises a breach of patient information occurring was interpreted from the data. These new key definitions were interpreted from the described experiences of the nurses themselves, as the trusted protector of patient information. Comparisons were made between the two provinces on the perceptions/experiences of nurses with regard to the security and privacy of electronic records compared to paper records. A trusted relationship builds between the nurse and the patient with regard to patient or health information. Family relationships were to be among the most challenging. Breaches were found to occur intentionally or unintentionally.

Findings and recommendations from this study will add to the knowledge-base of nursing and health care professional practice, ethics and informatics. The findings could also positively influence the personal attitudes of nurses towards patient information privacy.

ACKNOWLEDGEMENTS

It is often said that a journey of many miles starts with a step. I would like to express a depth of gratitude to my first wife, Adriana Jane Sackey, who the Lord has called to glory, for the tremendous encouragement she gave in taking this initial step. May her beautiful soul rest in peace. My sincere thanks also go to my two adult sons, Adrian and Emmanuel for “pushing” me along the way with their incessant asking of how things are going and making jokes about when

I would stop studying. I must say that I have been a source of encouragement to them in their academic pursuits as much as they have prodded me on my academic journey. I do appreciate them very much. My warm gratitude goes to my wife, Sandra, for being the great person that she has been to me. You have been nothing but a rock and support. I will forever be grateful for your nudging and company. You have travelled this journey before and clearly understand the synclines and anticlines along the way. Thanks for your incredible support and commitment.

I would like to take this opportunity to express my deepest gratitude to Dr. Arlene Kent-Wilkinson, who has been my supervisor and a solid rock from the beginning. It is still fresh in my memories how you encouraged me especially when I lost my first wife and at times felt like throwing in the towel. I am where I am today because of your tremendous encouragement and also, believing in me. You are a special person and have influenced my life in a very dramatic way forever. Thank you for your patience and gentle spirit. A big “thank you” to my committee members; Dr. Arlene Kent-Wilkinson, Dr. Keith A. Willoughby, Dr. David Burgess, Dr. Sandra Bassendowski, the late Dr. Jim Greer and Committee Chair Dr. Linda Ferguson for providing the necessary guidance and making meaningful contributions to my study. I do appreciate all of you.

I wish you all well as you travel this journey of life.

DEDICATION

The task of dedicating an endeavor is always a difficult one, given the many influences one has and continues to experience in life. The significance of dedication is also an important consideration. Therefore, this act of dedication cannot be done carelessly. I know that I have done some personal soul searching as well as look at society in coming up with dedicating this work to the very people who were the subject of the study.

Nurses are a dedicated group of individuals who work tirelessly to ensure our well-being. The current trend of world-wide events (Covid-19) would testify to this. I am dedicating this work in honor of nurses who work hard to keep us alive, often, to their peril. I also dedicate the work to Adriana Jane Sackey, who motivated me in many ways to do this study.

TABLE OF CONTENTS

	COVER PAGE	
	MEMBERS OF ADVISORY COMMITTEE	i
	PERMISSION TO USE	ii
	ABSTRACT	iii
	ACKNOWLEDGEMENTS	iv
	DEDICATION	v
	TABLE OF CONTENTS	vi
	LIST OF FIGURES	xi
	LIST OF TABLES	xii
	ABBREVIATIONS- List of All Acronyms	xiii
1.0	CHAPTER ONE: INTRODUCTION	
1.0	An Exploratory Study of Registered Nurses' Experiences in Patient Information Privacy and Security within the Provinces of AB and SK	1
1.1	Keywords	3
1.2	Background/Need for Research	7
1.2.1	<i>Regulatory Mandates</i>	8
1.2.2	<i>Personal Interests</i>	9
1.2.3	<i>Significance of Study</i>	10
1.3	Statement of the Problem/Research Question	10
1.3.1	<i>Statement of the Problem</i>	10
1.3.2	<i>Research Question</i>	11
1.4	Existing Literature	11
1.5	Regulatory Laws and Acts	12
1.6	Electronic Health Records (EHR)	13
1.7	Breaches to Patient Information Privacy	13
1.8	Practice Environment	14
1.9	Purpose and Relevance of the Study	14
1.10	Nursing Practice Regulated by Legislation	14
1.11	RN Role in Patient Information	15
1.12	Overview/Outline of Research	16
2.0	CHAPTER TWO: REVIEW OF RELEVANT LITERATURE	19
2.1	Literature Review Method	20
2.1.1	<i>Search Strategy</i>	20
2.1.2	<i>Inclusion/Exclusion Criteria</i>	21
2.1.3	<i>Results of Search</i>	21
2.1.4	<i>Data Search Limitations</i>	22
2.1.5	<i>Sources of Information</i>	22

2.2	Literature Review Results/Findings	23
2.2.1	<i>Patient Information Privacy and Security</i>	24
2.2.1.1	Patient Information; Introduction	24
2.2.1.2	Data, Information, and Knowledge	25
2.2.1.3	Patient Information	26
2.3	Information Privacy and Developments	27
2.3.1	<i>Privacy</i>	27
2.3.1.1	Managing Information Privacy	33
2.3.2	<i>Privacy Perceptions</i>	35
2.3.3	<i>Patient Information Accessibility</i>	41
2.3.4	<i>Historical Developments in Information Privacy</i>	46
2.3.5	<i>Privacy Frameworks</i>	51
2.3.5.1	Organization for Economic Co-operation and Development (OECD) privacy principles	51
2.3.5.2	Asia-Pacific Economic Cooperation (APEC)	53
2.3.5.3	Fair Information Framework	56
2.3.5.4	International Standardization for Organizations	57
2.3.6	<i>Ethical-Legal Environment of Privacy</i>	58
2.3.6.1	Feminist Ethics	71
2.3.6.2	Moral Distress	71
2.3.6.3	Ethical Dilemmas	72
2.4	Social Media, Nurses, and Information Privacy	75
2.5	Information Privacy Breaches	78
2.6	Electronic Health Records	86
2.6.1	<i>Electronic Health Records and Patient Information Privacy</i>	90
2.7	Nursing Roles and Patient Information Privacy	94
2.8	Gaps in the Literature	100
3.0	CHAPTER 3: METHODOLOGY	102
3.1	Worldview	102
3.2	Approach	103
3.2.1	<i>Interpretive Description</i>	103
3.2.2	<i>Other Approaches</i>	105
3.3	Conceptual Framework	109
3.3.1	<i>Components of the Conceptual Framework</i>	109
3.3.1.1	Experience	110
3.3.1.2	Registered Nurse	110
3.3.2	<i>Development of the Conceptual Framework</i>	111
3.4	Research Design	115
3.4.1	<i>Setting of the Study</i>	115
3.4.2	<i>Sampling Procedure/Strategy</i>	116
3.4.3	<i>Data Collection Procedure</i>	118

4.0	CHAPTER 4: DATA ANALYSIS	122
4.1	Purpose of Data Analysis	123
4.2	Ethical Consideration	125
4.3	Dissemination of Findings	126
5.0	CHAPTER 5: RESULTS	129
5.1	Purpose of Research	130
5.2	Demographic Statistics and Observations from the Study Participants	130
5.3	Definitions Emerging from the Data	132
5.4	Primary Research Question	134
5.5	Broad Themes and Subthemes (Dichotomous Themes)	135
5.6	Theme A – Patient Information Protection	136
5.6.1	<i>Protection Initiatives</i>	137
5.6.1.1	Intentional v. Unintentional	138
5.6.1.1.1	<i>Respect</i>	138
5.6.1.1.2	<i>Safety</i>	139
5.6.1.2	Expectations v. Realities	140
5.6.1.3	Regulatory Compliance v. Interpretation	141
5.7	Theme B – Patient Information Breach	142
5.7.1	<i>Intentional v. Unintentional</i>	142
5.7.2	<i>Attitudes towards Breach</i>	144
5.7.2.1	Why breaches occur	145
5.7.2.1.1	<i>Curiosity</i>	145
5.7.2.1.2	<i>Entertaining</i>	146
5.7.2.1.3	<i>Human Nature</i>	146
5.7.2.1.4	<i>Pressure from Patient's Family</i>	146
5.7.2.1.5	<i>Boredom</i>	148
5.7.2.1.6	<i>Lack of Education</i>	148
5.7.2.1.7	<i>Reaction v. Response</i>	149
5.7.2.1.8	<i>Action v. Inaction</i>	149
5.8	Theme C - Access to Patient Information	150
5.8.1	<i>Accessible (open) v. Restricted access</i>	151
5.8.2	<i>Sharing of Information v. Protection of Information</i>	153
5.8.2.1	Social Media	157
5.9	Theme D - Education of Patient Information	158
5.9.1	<i>Awareness v. Ignorance</i>	159
5.10	Theme E - Nursing Practice	160
5.10.1	<i>Professional Obligation v. Human Nature</i>	161
5.10.2	<i>Challenges v. Consequences</i>	165
5.10.2.1	Privacy Infrastructure	166
5.10.2.2	Pressure from the Patient's Family	167
5.10.2.3	Consequences	169

5.10.2.4	Safe v. Unsafe Practices	170
5.10.2.5	Trust v. Mistrust	172
5.11	Theme F - Electronic Records and/or Paper Records	173
5.11.1	<i>Secure v. Vulnerable</i>	174
5.11.2	<i>Benefits v. Pitfalls of Electronic Records</i>	178
5.11.3	<i>Benefits v. Pitfalls of Paper Records</i>	181
5.12	Theme G - AB and SK Health Regions	183
5.12.1	<i>Similarities v. Differences in AB and SK</i>	185
5.12.2	<i>Resources v. Limited Resources</i>	186
6.0	CHAPTER 6: ANALYSIS AND DISCUSSION	187
6.1	Theme A – Patient Information Protection	188
6.1.1	<i>Subtheme: Protection Initiatives</i>	194
6.1.2	<i>Subtheme: Intentional v. Unintentional</i>	195
6.1.3	<i>Subtheme: Safety</i>	196
6.1.4	<i>Subtheme: Expectations v. Realities</i>	198
6.1.5	<i>Subtheme: Regulatory compliance v. Interpretation</i>	200
6.2	Theme B – Patient Information Breach	202
6.2.1	<i>Subtheme: Intentional v. Unintentional Breaches</i>	203
6.2.2	<i>Subtheme: Attitudes towards Breach</i>	205
6.2.2.1	Seriousness	205
6.2.2.2	Consequences	205
6.2.2.3	Sharing	205
6.2.2.4	Saying too Much	206
6.2.2.5	Hesitation to Report	206
6.2.2.6	Famous Person Situation; Breaches More Likely	206
6.2.2.7	Willingness to Share Challenges	207
6.2.3	<i>Subtheme: Why Breaches Occur</i>	207
6.2.3.1	Curiosity	207
6.2.3.2	Human nature	209
6.2.3.3	Entertainment	209
6.2.3.4	Pressure from Patient's Family	209
6.2.3.5	Boredom	210
6.2.3.6	Lack of Education	210
6.2.3.7	Reaction v. Response	211
6.2.3.8	Actions v. Inaction	211
6.2.3.9	Venting	213
6.3	Theme C – Access to Patient Information	213
6.3.1	<i>Subtheme: Sharing Information v. Protection of Information</i>	215
6.3.2	<i>Subtheme: Social Media</i>	217
6.4	Theme D – Education of Patient Information	219
6.5	Theme E – Nursing Practice	223

6.5.1	<i>Subtheme: Professional Obligation v. Human Nature</i>	226
6.5.2	<i>Subtheme: Challenges v. Consequences</i>	228
6.5.2.1	Privacy Infrastructure	229
6.5.2.2	Pressure from Patient's Family	230
6.5.2.3	Consequences	231
6.5.2.4	Safe v. Unsafe Practices	232
6.5.2.4.1	<i>Nurses' Discretion</i>	232
6.5.2.4.2	<i>Audits</i>	233
6.5.2.4.3	<i>Electronic v. Paper Records</i>	233
6.5.2.4.4	<i>Effectiveness and Efficiency</i>	234
6.5.2.4.5	<i>Duplicate Patient Information</i>	234
6.5.2.4.6	<i>Education/Patient Information Privacy</i>	235
6.5.2.5	Trust v. Mistrust	235
6.6	Theme F – Electronic Records and/or Paper Records	235
6.6.1	<i>Subtheme: Secure v. Vulnerable</i>	235
6.6.2	<i>Subtheme: Benefits v. Pitfalls of Electronic Records</i>	238
6.6.3	<i>Subtheme: Benefits v. Pitfalls of Paper Records</i>	239
6.7	Theme G – AB v. SK Health Regions	240
6.7.1	<i>Subtheme: Similarities v. Differences in AB and SK</i>	240
6.7.1.1	Resources v. Limited Resources	241
7.0	CHAPTER 7: RECOMMENDATIONS, LIMITATIONS, FUTURE RESEARCH OR IMPLICATIONS FOR PRACTICE AND CONCLUSION	244
7.1	Recommendations and Implications for Practice	244
7.1.1	Academic	245
7.1.2	Policy Makers' Decisions	247
7.1.3	Support for Educational and Practice Training Resources	248
7.1.4	Practitioners	251
7.2	Limitations	252
7.3	Summary of Findings (Implications for Practice)	253
7.4	Conclusion	257
7.4.1	Key Definitions Interpreted/co-Constructed from Data	257
7.4.2	Significance of the Study	261
	REFERENCES	264
	APPENDICES	294
	Appendix 1: Behavioral Research Ethics Board Certificate of Approval	294
	Appendix 2: Invitation to Participate in the Research Study	296
	Appendix 3: Consent to Participate in a Research Study	298
	Appendix 4: Demographic Questions	301
	Appendix 5: Interview Guide	302

LIST OF FIGURES

	Figure 3.1: Interactions Between Components of Conceptual Framework that Generate a Nurse's Patient Information Privacy and Security Experiences	113
	Figure 6.1: Interactions Between Components of Conceptual Framework that Generate a Nurse's Patient Information Privacy and Security Experiences	191
	Figure 6.2: Reality of Patient Information Flow	193

LIST OF TABLES

	Table 2.1: Country Comparison of Privacy Acts	64
	Table 5.1: Demographic Statistics of Study Participants (AB and SK)	130
	Table 5.2: Definitions beginning to be Co-Constructed from the Data	132-133
	Table 5.3: Themes and Sub Themes	135-136
	Table 5.4: Timeline – All Acts Related to Privacy and Security	183
	Table 7.1: New Definitions Interpreted-Co Constructed from the Data	262

ABBREVIATIONS

List of All Acronyms Used in Dissertation/Manuscript

Acronym	Name of Act, Organization, or Institution	Page(s) found in Manuscript
AACCN	American Association of Critical Care Nurses	68, 251
APA	American Psychiatric Association	87, 251
ASBH	American Society for Bioethics and Humanities	69–70, 251
APEC	Asia-Pacific Economic Cooperation	7, 48, 50–55, 252
CASN	Canadian Association of Schools of Nursing	93–94210, 254
CBC	Canadian Broadcasting Corporation	8, 13, 22, 31–32, 253–255, 265
CHI	Canada Health Infoway	12, 35–37, 85, 210, 251
CNA	Canadian Nurses Association	27, 30, 58, 60, 105, 213, 255
CNPS	Canadian Nurses Protective Society	12, 73, 238, 255
CDO	Care Delivery Organization	82, 262
CARNA	College and Association of Registered Nurses of Alberta	iii, 26, 88, 209, 245, 256–257
EHR/EMR	Electronic Health Records /Electronic Medical Records	5, 6, 12, 39–40, 82–87, 92, 94, 164, 254, 260, 262, 267
FIP	Fair Information Practices	33, 45, 58, 260
FIPPA	Freedom of Information and Protection of Privacy Act, 2000	58, 174
GT	Grounded Theory	101
HEW	Health, Education, and Welfare	54
HIA	(AB) Health Information Act (HIA), 2000	iii, 7, 8, 10–11, 14, 18, 21, 27, 127, 174, 178, 261
HIPA	(SK) Health Information Protection Act, 2003	iii, 4, 6–8, 10–11, 14, 18, 21, 59, 174, 178, 261
HIPAA	(U.S.) Health Insurance Portability and Accountability Act, 1996	57, 59, 61, 88, 127, 204, 205, 256
NHSIA	(England & Wales) National Health Service Information Authority	58
HSCA	(England & Wales) Health and Social Care Act, 2003	58
ITA	Inductive Thematic Analysis	100–102
ISO	International Standards Organization	49, 54, 263

IBN	Iowa Board of Nursing	73, 263
NIST	National Institute of Standards and Technology	84, 267
NPR	National Public Radio	78,
OPC	Office of the Privacy Commissioner of Canada Acts	35, 36-39, 44, 47, 64, 174, 269
PA-US	(U.S.) Privacy Act, 1974	60
PA-C	(CA) Privacy Act, 1982	58
PIAG	(England & Wales) Patient Information Advisory Group	58
PHIA	Personal Health Information Act, 1997	61
PHIA	Personal Health Information Act (PHIA), 1957	61
PHIPA	(ON) Personal Health Information Protection Act, 2004	58, 81, 174, 255
PHR	Personal Health Record	6, 12, 82, 83, 262
PIPEDA	Personal Information Protection and Electronic Documents Act, 2003	47, 58, 61, 81, 174
PAPHR	Prince Albert Parkland Health Region	77
PPA	<i>Privacy Protection Act</i>	174
PRC	Privacy Rights Clearinghouse	12, 82-84
PRCCDB	Privacy Rights Clearinghouse's Chronology of Data Breaches	75
RN	Registered Nurses	1-3, 10, 12, 14, 18, 21, 26, 68, 72, 79, 87, 103, 109, 116, 124–125, 175, 185, 207, 208, 225, 226, 236, 248, 250, 264, 266–267, 275, 277, 280
RNAO	Registered Nurses Association of Ontario	105, 271
RCMP	Royal Canadian Mounted Police	77
RCN	Royal College of Nursing	105, 212, 213, 273
SRNA	Saskatchewan Registered Nurses Association	1, 3, 209, 273
SBN	Security Breach Notification	55
USDHEW	U.S. Department of Health, Education, and Welfare	54
USNCSBN	U.S. National Council of State Boards of Nursing	12
VIPS	Very Important Personalities	25
WABE	Washington Association for Bilingual Education	79
WHO	World Health Organization	71, 92, 272, 278

CHAPTER 1 – INTRODUCTION

An Exploratory Study of Registered Nurses’ Experiences in Patient Information Privacy and Security within the Provinces of AB and SK

Patient information privacy and security is important to individuals as well as governments. As a result, there are several Acts and regulations to protect such information. Nurses play a major role in the collection, dissemination, and exchange of patient information.

While a nurse’s primary role is to protect the health of the patient, she or he needs to comply with stipulated Acts and regulations. Therefore, it is not difficult to imagine how complicated the nurse’s work environment could quickly become. Little is known about the experiences of nurses in patient information privacy and security. Finding out how nurses feel, their thoughts, knowledge, and understanding as they comply with patient information privacy and security regulations was most interesting. Some exposition from the nurses themselves could be the first step towards making the necessary changes to improve the nurse’s work environment.

Patient information privacy and security may mean different things to different people. If not properly controlled, patient information could end up in the hands of unauthorized individuals, resulting in a breach of the patient’s privacy and security. A breach could adversely impact the patient’s status at work, personal relationships, result in discrimination, and have many other negative effects. Healthcare workers such as registered nurses (RNs) are obligated to ensure the privacy and security of patient information in their regular discharge of duties. According to the Saskatchewan Registered Nurses Association (SRNA, 2015), registered nurses are self-regulated

health care professionals who work autonomously and in collaboration with others. Throughout this dissertation, the term “nurse” means RN.

Each nurse-patient or nurse-nurse interaction in the context of patient information privacy and security may present its own challenges to learn from or opportunities to do better. Patient information privacy and security experiences as told by the nurses resulted in some interesting discoveries by the researcher. As nurses comply with privacy and security regulatory mandates, they follow stipulated rules and policies in order to safeguard patient information. As patient information is received from patients, nurses, and other health care workers or units, this information exchange makes for a complex system of information flows. This could be exacerbated by the often unpredictable work environments and decision-making processes that has become part of nursing care. How restricting are privacy and security mandates? How well-informed are nurses regarding such mandates? How do nurses deal with patient information privacy dilemmas that confront them on a daily basis? Why do health record breaches appear to be a commonplace? These are a few questions that my exploratory qualitative research sought to gain insights and perspectives to inform possible further research.

Although a lot of research has been conducted in the field of information privacy and security, preliminary review of the literature indicates that there is a gap and dearth in research that focus on patient information privacy and security. In particular, studies that explore the experiences of nurses in patient information privacy and security are almost absent, at least from the initial literature search. The proposed research study will help elucidate this important area of information privacy and security for which little is known.

1.1 Keywords

Patient information privacy and security may mean different things to different people.

For clarity the following terms pertinent to this study are defined or described: Registered nurse (RN), patient, patient information system, electronic record systems, privacy, security, breach and qualitative. The definitions cited for the most part are from professional associations and government agencies.

Registered Nurse (RN)

The Saskatchewan Registered Nurses Association (SRNA) is the largest profession-led regulatory body in SK with more than 12,000 members (SRNA, 2020). Established in 1917 by the provincial legislature the SRNA is accountable for public protection by ensuring members are competent and promotes the professional interest of its members in the public interest (SRNA, 2020). The registered nurse's scope of practice is specifically outlined in the Registered Nurses' Act, 1988 (Statutes of Saskatchewan [SK], 1988).

In Alberta (AB), the College and Association of Registered Nurses of AB (CARNA, 2020a) is the professional and regulatory body for 37,000 registered nurses and nurse practitioners throughout AB. The CARNA is mandated to define and uphold the standards of safe and ethical nursing practice as legislated under the Health Professions Act (CARNA, 2020a). In May 1999, the AB passed the Health Professions Act to regulate all 30 self-governing health professions. This legislation requires all health professional colleges to follow common rules to investigate complaints and set educational and practice standards for registered members (AB Health & Wellness, 1999).

Registered nurses (RNs) and other professional healthcare workers are obligated to ensure the privacy and security of patient information in their regular discharge of duties (CARNA, 2020b).

Throughout this dissertation, the term “nurse” means RN.

Patient

A patient has been defined as a person under health care (Shiel, 2021). According to this author, the person may be waiting for this care or may be receiving it or may have already received it. Same author points out that, there is considerable lack of agreement about the precise meaning of the term "patient." Several terms are used to describe persons receiving services in the health care system: consumers, patients, etc. For the purpose of this study the term patient was used throughout.

Patient Information

The meaning of “patient information” appears to be clarified by legislation. Sections 2(m) and 2(q) of the SK *Health Information Protection Act (HIPA)*, effective since 2003 (Government of SK, 2020a) have defined personal health information to include:

(i) information with respect to the physical or mental health of the individual; (ii) information with respect to any health service provided to the individual; (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; (iv) information that is collected: (A) in the course of providing health services to the individual; (B) or incidentally to the provision of health services to the individual; and (v) registration information, that is, information about an

individual that is collected for the purpose of registering the individual for the provision of health services (p. 5).

Patient Information Management System

A patient information system (PIS) is also often referred to as patient information management system (PIMS) which is, essentially, a data management system that facilitates processing of patient information. When done properly, analysis of data in patient information systems can lead to new insight and understanding of health and disease, both chronic and acute.

Electronic Record Systems/Paper Records

According to HealthIT (2018), EHRs are real-time, patient-centered records. The EHRs make information available instantly, whenever and wherever it is needed. HealthIT further elaborate that EHRs bring together in one place everything about a patient's health. The authors also add that EHRs contain information about a patient's medical history, diagnosis, medications, immunization dates, allergies, radiology images, and lab and test results. In addition, EHRs: offer access to evidence-based tools that providers can use in making decisions about a patient's care; automate and streamline providers' workflow; increase organization and accuracy of patient information; and, support key market changes in payer requirements and consumer expectations. Paper records systems are typed or hand written notes compiled in categories of every aspect of the personal health information of patient (HealthIT, 2018, 2019, 2020). The two systems will be compared to determine benefits and limitations.

Electronic Health Records (EHR)/ Electronic Medical Records (EMR)

Electronic Health Records (EHRs) capture patient information in digital format and make the information available to other healthcare stakeholders (Angst & Agarwal, 2009). The EHRs represent the ability to easily share medical information among stakeholders and to have a patient's information follow him or her through the various modalities of care engaged by that individual. An EHR may draw on health information sources such as EMRs, drug repositories, centralized lab sources, and other point of service applications over many encounters to assemble a complete health record about a patient (Ludwick & Doucette, 2009).

Electronic Medical Records (EMR) are electronic patient records that are created and maintained by one care delivery organization and includes patient medical history, clinical documentation, medications, laboratory, and radiology test results (Parks et al., 2011).

The terms electronic medical records (EMR) and electronic health records (EHR) are often used interchangeably but the literature suggest that they have different meanings (Garets & Davis, 2006). Another term that is often confused with electronic health records is personal health record (PHR). A PHR is a collection of health-related information that is documented and maintained by the individual it pertains to.

Privacy

In the Health Information Acts in Canada, privacy is defined with a legal context and adapted to meet local needs. For example, in the province of SK, HIPA, 2003 defined privacy as the right to consent and revoke consent to use and disclosure, the right to prevent access to a comprehensive health record, the right to be informed by trustees about anticipated uses and disclosures, and the right to be informed about disclosures without consent (Government of SK,

2020a, 2020b).

Breach

In a legal sense, The Law House (2019) asserts that a breach occurs when you do something that you were required by the court to do, or not do. A breach is the breaking of a rule or law or the upsetting of a normal and desired state. An information privacy breach could therefore be defined as any act that is contrary to established information privacy laws, rules, regulations, standards, and similar mandates designed to protect information privacy.

Experience

Daher et al. (2017) have painted a casual meaning of “experience” in which they claim that “ In ordinary life, our experiences about the world, others, and us usually do not involve questions or doubts at first; on the contrary, many times they are taken for granted as seamless elements of the processes we call routines” The study sought to gather and understand the meanings nurses constructed based on their already-lived, past “event”. It is this already-lived events that this study captured as “experience.

Qualitative

A qualitative measure relates to assessing by the quality (size, appearance, value, etc.) of something. Qualitative data which was used in this study is descriptive, and can be observed but not measured (QuestionPro, 2020).

1.2 Background/Need for Research

There is a need for research in patient information privacy and security as many sectors have expressed a concern for the safety of personal health care information. Background information is cited on regulatory mandates by health care organizations and governments; my

personal experience or interest, and the significance of this study resulted in choosing this topic for my research topic.

1.2.1 Regulatory Mandates

Patient information privacy and security is a concern shared by individuals, healthcare organizations, and governments around the world. Ball et al. (2007) have reported a study conducted in the United States in which two-thirds of American consumers expressed serious concerns about the privacy of their personal health information.

The two health information acts applicable for the provinces of SK and AB are the SK *Health Information Protection Act (HIPA)*, enacted in 2003 (Government of SK, 2020a, 2020b), and the AB *Health Information Act (HIA)*, enacted in 2000 (Government of AB, 2020a, 2020b). The AB *HIA* and the SK *HIPA* are constantly undergoing changes. In an article published by the Field Law (2020), Yu has indicated that the HIA is constantly undergoing changes in many areas including disclosure of health information where significant risk of harm exists, refusal to conduct inquiry, increase in fines for offences, and many others. Also, in a recent publication, the Canadian Broadcasting Corporation (CBC, 2020b) mentioned that, in a letter sent to the health minister, AB's privacy and information commissioner suggested ten ways the HIA could be improved.

The changes are ongoing with a significant change effective August of 2018 put in place mandatory breach reporting and provides guidance for such reporting (Glowingwlg.com, 2018). Changes to the SK *HIPA* is happening but at a slower pace than in AB. This slower pace has been exemplified in an article written by Latimer (2018) of CBC, in which the author expressed concern about the privacy commissioner having to wait two years for amendments to health

information privacy laws. As a result of the dynamic nature of *HIA* and *HIPA*, it is often easier to track the changes that are occurring over time. However, at the date of this writing, both information acts, the AB *HIA*, and the SK *HIPA* have been updated to 2020 with amendments as per their statutes (Government of AB, 2020a, 2020b; Government of SK, 2020a, 2020b).

1.2.2 Personal Interests

The study was not only as a result of the concern governments and individuals have for patient information privacy and security as mentioned above; my *personal interest* in this research was also partly spurred by my involvement in education administration while working in the United States as the dean of academic affairs of a tertiary institution. I was responsible for ensuring that academic programs were achieving their desired outcomes. The college I worked for started a nursing program that required students to do clinical hands-on exercises in a hospital as part of the learning process. I had the opportunity to visit the students on supervisory routine visits. The general observations I made during such visits regarding patient information privacy and security had me asking myself a number of questions about the significance of privacy regulatory compliance and nursing practice.

I have always wondered about the nurse's role as a caregiver and as a confidant, and more importantly, their obligation to protect patient information. What are their thoughts regarding patient information privacy and security in general? What concerns do they have regarding the methods and procedures in place to protect patient information? How do nurses feel about patient information regulatory compliance and related issues? These questions and recent information privacy breaches involving nurses had me searching for the RN's perspective on patient information privacy and security from the available literature. Although much has

been written about information privacy and security in the health care sector, I wondered how much has been done and the ease of finding or accessing work in the specific area of patient information privacy and security from the viewpoint of the RN. Was it in the ‘grey’ literature of health care region literature as opposed to the ‘academic or published’ literature?

1.2.3 Significance of Study

The outcome of a research study of the experiences of RNs with regard to patient information privacy and security will add to the scholarly nursing education research and literature. This may be particularly important, given the questioned accessibility or notable paucity in the literature in this area. Results of the research will help provide direction for further research to improve policy and decision making in patient information privacy and security for RNs. The study provided evidence for a “bottom-up” approach to the formulation and implementation of privacy and security policies and guidelines. Ideas or plans that are informed by its participants are likely to be better received by the participants, and more likely to succeed.

This could subsequently lead to better nursing practice.

1.3 Statement of the Problem/Research Questions

The issues that formed the basis for the proposed research are briefly discussed in this section. Research questions pertinent to the problem statement are posed and briefly discussed as well.

1.3.1 Statement of the Problem. This research study specifically explored the experiences of medical-surgical/critical care registered nurses with regard to patient information privacy and security in AB and SK. Experience in the context of the proposed study is: “the actual living through an event... the real life as contrasted with the ideal or imaginary ... The sum total of the conscious events which compose an individual life” (Erlich, 2008, p. 1126).

1.3.2 Research Question(s). The purpose of the research was to gain better understanding of the experiences of RNs in patient information privacy and security in AB and SK health regions. Specific goals included capturing rich insights and concepts related to perceptions, feelings, reflections, thoughts, and even apprehension and comprehension. Such insights will lead to understanding what is important or not important to RNs, ascertain specific implications, provide clues to understanding some existing behavior patterns, and inform future research.

Due to the exploratory nature of my study, the primary research question was broadly stated as “what are the experiences of medical-surgical/critical care registered nurses as they comply with the regulatory health information acts of *HIA* (Government of AB, 2020a, 2020b) in AB and *HIPA* (Government of SK, 2020a, 2020b) in SK in their day-to-day nursing practices in a hospital?” Other relevant questions related to the primary research question were “what meanings do nurses bring to patient information privacy and security practices?”, “are nurses concerned about the expectations mandated by Health Information Acts?”, “how adequate is the preparation nurses receive in the area of regulatory compliance?” The research was designed and conducted to ensure that the research question was answered as completely as possible.

1.4 Existing Literature

Although a lot of research has been conducted in the field of information privacy and security, preliminary review of the literature indicated that there is a gap and dearth in research that focuses on patient information privacy and security. In particular, studies that explore the experiences of nurses in patient information privacy and security are almost absent, at least from

the initial literature search. The proposed research study helped to elucidate this important area of information privacy and security for which little is known.

Existing literature in healthcare privacy and security that are written with RNs in mind often tend to be prescriptive in nature, and lack the perspective of the nurses. They generally consist of laws and regulations, practice standards, ethics, best practices, policies, and frameworks. There appears to be continued high expectations for nurses to comply with mandatory regulations and use of guidelines. However, in the published literature, not much has been done to attempt to understand the nurse's "world" of regulatory compliance and the ever-changing practice environment for nurses.

1.5 Regulatory Laws and Acts

The SK, *HIPA* (Government of SK, 2020a, 2020b), and the AB, *HIA* (Government of AB, 2020a, 2020b), state a patient's privacy rights pertinent to the two provinces that healthcare workers including RNs need to be aware of. There are also legal definitions of what constitutes patient information that RNs need to assimilate and work with. Information privacy and security policies and procedures that RNs have to be familiar with, have received considerable attention in the past and continue to be important to nursing practice.

In their "info LAW" publication, the Canadian Nurses Protective Society (CNPS, 2008) called on nurses to be mindful of their legal and ethical obligations to keep health information confidential. The Society pointed to several sources to obtain relevant information. These sources included federal/provincial/territorial legislation governing personal health information, regulated health profession, health facilities, health insurance, occupational health, and privacy; court decisions; the Canadian Nurses Association's (2008, 2017) *Code of Ethics for Registered*

Nurses; provincial/territorial nursing practice standards; institutional confidentiality agreements and policies; and publications by the Health Information Management Association and Accreditation Canada (CNPS, 2008). Current editions of the suggested sources should provide useful and pertinent information.

Larsson et al. (2011) established in their study of patients' perceptions of nurses' behavior that influence patient participation in nursing care, that it was important for the nurse to act as a mediator of contacts. This role means facilitating patient-to-patient, patient-to-family, and at times patient-to-physician communications. The implication here is that at any point in time, the nurse is receiving and sharing a multitude of information, being careful to decipher what to share and what not to, in order to respect the patient's privacy.

1.6 Electronic Health Records (EHR)

The EHR initiatives continue to be important in Saskatchewan and Alberta. Challenges that nurses face in the EHR system may range from mere use of disparate terminologies for the same tasks or processes to technological know-how in day-to-day operations (Canada Health Infoway [CHI], 2008). As noted by the CNPS (2008), computerization in health care raises major legal concerns related to the confidentiality of health records because of the potential for unauthorized access and data sharing. Although using computers is the norm in many hospitals, health care centers and physicians' offices, this technology does not change a patient's right to privacy of their health information.

1.7 Breaches to Patient Information Privacy

Several cases of patient information privacy breaches involving nurses have been reported in the media (CBC News, 2012; HealthCare IT News, 2013; North Bay Local News,

2011). In many of these cases, the context of the incidents as reported by the media are often narrowly defined. A forum is needed to hear the stories of nurses that would put some of the breach incidents in perspective. The purpose of such a forum is not to justify wrong doing, but provide a view by which to mediate harsh judgments by society or the legal system. In summary, it could be said that the nurse's practice environment consists of information that needs to be acted upon with care. Notably, the healthcare environment is in a state of constant flux.

1.8 Practice Environment

The state of affairs with regard to a nurse's patient information privacy and security endeavors, as described above suggests that a nurse's practice environment continues to be complex. The impact of such complexity on how nurses navigate patient information privacy and security, among other things, has not been well documented. Available literature is almost silent about this. This research study provided the opportunity to delve into the experiences of RNs to discover what they have observed, encountered, or undergone in the course of time, in the context of the complex practice environment described earlier.

1.9 Purpose and Relevance of the Study

The purpose of this exploratory research study was to gain better understanding of the experiences of RNs with regard to patient information privacy and security within the AB and SK health region(s). Specific goals included capturing rich insights and concepts that lead to understanding what is important or not important to nurses, ascertain specific implications, and inform future research.

1.10 Nursing Practice Regulated by Legislation

In Canada, nursing practice is regulated by legislation. Mandatory compliance with patient information privacy and security regulations has brought with it the need for RNs to read, understand, and interpret the law. This could be overwhelming. In SK for example, the *HIPA* has nine major parts that cover: part i, preliminary matters; part ii; the rights of the individual; part iii, duty of trustees to protect personal health information; part iv, limits on collection, use, and disclosure of personal health information by trustees; part v, access by individuals to personal health information; part vi, review and appeal; part vii, commissioner; part viii, general; and part ix, transitional consequential amendments, and coming into force (Government of SK, 2020a, p. 2). The AB *HIA* has similar worded categories or parts (Government of AB, 2020a).

The language in which the Act was written, and the ambiguity often associated with statements in such Acts could constitute a major source of confusion for many. The abundance of regulation- and policy-related questions asked by nurses to other nurses on social media such as Facebook and the likes seeking clarification from one another is perhaps evidence of the lack of understanding and clarity of the regulations they are supposed to work with. The role of technological advances that have made electronic health records inevitable and the challenges in the proper use of these technologies can be a source of pressure RNs have to deal with.

1.11 RN Role in Patient Information

Registered nurses (RNs) have a significant presence in the collection, storage, retrieval, and sharing of patient information in the health care sector. Their impact and contribution to patient information privacy and security endeavors cannot be underestimated. The exploratory study which looked at the RN's actual living through patient information privacy and security events

and practices should provide a platform for understanding some of the issues confronting nursing practice. The themes and concepts that evolve from analysis of data collected for this study should also provide guidance to the selection and design of subsequent detailed research in the area of patient information privacy, security, and nursing practice.

1.12 Overview/Outline of Research

Chapter 1 defines or describes key terms used in the study to provide context and ensure a common understanding of these terms. The need for this research section identifies the significant regulatory laws and acts for health information in AB and SK. A background to the research study is provided and how it emerged. The significance of the research study is also discussed in some detail. A problem statement for the research is also made in this section.

Pertinent questions that shed more light on the problem statement are asked and briefly discussed. The purpose of the study is subsequently stated and explained to include what the research study seeks to achieve. Finally, chapter 1 concludes with a brief summary of chapters 1 and an overview of what is to come in chapters 2 through to chapter 7.

Chapter 2 provides the literature search strategies used described in detail. This description ends with statement(s) of limitation(s) encountered during the literature search. A major part of this section includes review of pertinent literature and presentation of findings. Sources of specific information are also mentioned here. This section draws on current research studies, previous and future research to identify existing gaps in the area of patient information privacy and security. Also important in this section is a brief description of how the proposed research would contribute to closing existing gaps in the literature.

Chapter 3 describes the methodological approach used for this research. The section begins with a discussion on the worldview the researcher brings to the research and the philosophical underpinnings. Epistemological perspectives will also be briefly discussed. The conceptual framework used in this research will be described, followed by a discussion of the research design. Qualitative research method will be described in detail, as this is the preferred design for my research. The setting for the study, sampling procedure or strategy, and sampling selection criteria will be thoroughly discussed in this section. Data collection procedure, data trustworthiness and analysis will be described as well. Ethical considerations and dissemination of findings are also discussed in chapter 3.

In chapter 4, data that were collected are organized, reviewed, transcribed and interpreted to provide the information being conveyed. Data analysis is the main purpose of chapter 4.

Coding of the information using documented methods follow data organization, review, transcription, and interpretation. Transcripts are carefully read again to ensure that important meanings are noted. Categories, themes, and subthemes are then sifted. The coding process allows me to create and develop abstractions from the data collected. Analysis is done manually, to allow me to immerse myself in data analysis. Attention is also given to journaling my activities. Due consideration is given to ethical matters and the necessary procedures followed.

Protocols for informed consent are followed as well, and participants treated with respect. Dissemination of the findings is done with the necessary care and not done in a hurry to register any claims.

Chapter 5 primarily consists of reporting the results of the study. Responses from the interviewees are presented in their raw forms, including comments associated with the results

and supporting direct quotes from the interviewees. Themes that emerged as a result of the study are noted and reported. Other unanticipated outcomes are reported as well.

In chapter 6, a detailed analysis of the results is provided. The themes and subthemes are further elaborated upon. The thoughts, perceptions, feelings, etc. captured from the nurses in the study are critically looked at, and contextualized. Some light is also shed on certain behaviours by nurses in relation to patient information privacy, what precipitated such behaviours without being judgmental. Personal experiences expressed by the nurses in view of the challenges they faced in patient information privacy and security have been “dissected” to provide useful

recommendations later.

Conclusions, recommendations and limitations to the study are included in chapter 7. The final chapter looks at what was learned during the study and the contributions the findings make to patient information privacy and security in the nurse’s “practice world”. Chapter 7 includes recommendations and their implications for practice, suggestions for future research, and some thoughts for policy decision makers. The study’s implications for nursing education and training are mentioned in this chapter. Limitations in the study are also indicated in this chapter.

CHAPTER II – REVIEW OF RELEVANT LITERATURE

Nurses constitute a significant proportion of healthcare professionals, and are the largest stakeholders that collect, use, transfer, and store patient information whether in paper or electronic form. Their impact on the privacy and security of such information cannot be ignored.

My research study was an exploratory study of RNs experiences in patient information privacy and security within the provinces of AB and SK. This study examined the involvement, skills, practices, understanding, know-how, proficiencies, concerns, and familiarities of nurses in patient information privacy and security.

The primary research question foundational to the literature review was broadly stated as: “what are the experiences of medical-surgical/critical care registered nurses as they comply with the AB *Health Information Act (HIA)* (Government of AB, 2020a, 2020b) and the SK *Health Information Protection Act (HIPA)* (Government of SK, 2020a, 2020b) in their day-to-day nursing practices in a hospital?” This research is only a part of the broad issues in patient information privacy and security. Some background and historical perspectives will therefore be provided as part of the literature review.

A good literature review has only one clearly defined goal, to make the case for the proposed study (Sandelowski & Barroso, 2003). To this end, relevant literature on work that has been published were reviewed. Identifying work done on patient information privacy and security in nursing helped situate the proposed research study. The literature review method used is presented next.

2.1 Literature Review Method

This section outlines the approach used for the literature review. Challenges faced during the data search are described, and sources of information used during the literature review are provided.

2.1.1 Search Strategy

Electronic searches were conducted using a wide variety of search terms individually and in combination. The terms used in the search included patient information, patient information privacy, patient information privacy in AB, patient information privacy in SK, patient information security, nurse involvement in patient information privacy, electronic health record privacy, electronic health record security, and nurse experience in patient information privacy. Articles in several databases were searched. The databases included Medline/PubMed, CINAHL, ERIC, and the Cochrane Library. Searches were also conducted using Google-Scholar and public libraries. The searches that were done through university library systems were done with the assistance of librarians. Public library searches were completed with occasional help from librarians. The search had the object of identifying both published and unpublished studies. Calls were also made to pertinent associations/society, sourcing for published or unpublished work. Searches using author names from the initial search results were conducted subsequently. In addition, literature from my personal collection of seminal information privacy and security were used.

The search covered the period between 1990 and 2018 as patient information privacy and security actually began to get noticeable attention in the early 1990s and has since gained momentum. In all the databases searched, individual words and combinations were used as

strings to ensure thoroughness. The Boolean operands “AND” and “OR” were also used extensively to broaden and/or narrow the search. Wildcards were also used. Records for all relevant articles written in English language were obtained for further consideration. Bibliography for retrieved articles considered useful were also searched for materials such as presentations and reports.

2.1.2 Inclusion/Exclusion Criteria

In all, 720 items were identified after performing the search described above. Most were articles from databases with a few unpublished articles and books from other sources. The article titles, keywords, and abstracts were screened. The initial inclusion criteria was that the article had to be a study (with data) conducted for the sole purpose of the involvement of nurses in patient information privacy and security. The criteria was subsequently broadened to include articles that described in some detail, patient information privacy and security with nurses at the focal point, or principles with substantial useful information for nursing practice but not necessarily supported with data. Articles that addressed general healthcare practitioners and did not explicitly mention nurses in the areas mentioned above were compared with those written primarily for nurses to ascertain eligibility for inclusion. To be included, such articles had to have substantial (about 80-90%) content applicable to nurses. Based on the inclusion criteria and after removal of duplicates, 240 articles were considered for further detailed reading of abstracts.

After reading the abstracts, 12 articles were included in the review and their full-text read.

2.1.3 Results of Search

In all, 73 articles, books, reports were identified. The full text of articles and reports were read.

2.1.4 Data Search Limitations

Most of the articles (about 15-20%) were written with practice standards, guidelines, regulation, or ethics background. The dominance of privacy concerns was obvious. Security issues were addressed minimally. Almost all of the articles seemed to have been written for registered nurses. Also, a significant number of the articles had American content. Important to point out is that no study or article was found that matched the study topic for which the systematic literature review was conducted. With regard to the research question of “what are the experiences of medical-surgical registered nurses as they comply with the AB *HIA* (Government of AB, 2020a, 2020b) and the SK *HIPA*, (Government of SK, 2020a, 2020b) in their day-to-day nursing practices in a hospital”, several useful articles were available. However, most of the articles only addressed some aspects of the research question. The articles together made for a meaningful exploration of nurses’ experiences in patient information privacy and security.

2.1.5 Sources of Information

Information used in this literature came from several sources. These sources include mainly published and in some cases non-published articles. The primary source is peer reviewed journals and articles mainly from the healthcare and information technology disciplines. Healthcare publications used come from organizations such as the Academic Emergency Medicine, Biomedical Central Medical Informatics, European Federation for Medical Informatics, Nursing for Women’s Health, Nursing Ethics, *Journal of the Medical Informatics Association*, Nursing Standard, *Journal of Clinical Nursing*, and Evidence Based Nursing. Information has also come from articles and journals in nursing association publications as well as boards of nursing, government organizations like the Office of the Privacy Commissioner, and

non-governmental organizations such as the Privacy Rights Clearinghouse. Some of the information included in this review have been obtained from pertinent textbooks. As mentioned earlier, personal seminal material were used as well. Information was also gleaned from media sources such as CBC, etc.

2.2 Literature Review Results/Findings

This section discusses some rudiments in the literature of information privacy and security foundational to understanding patient information privacy and security in the context of nursing practice. An overview of historical developments in information privacy and security is described in order to provide perspective. Nursing and the use of patient information does not occur in a vacuum. This section therefore discusses issues that affect nursing practice and patient information privacy and security such as the ethical-legal environment of information privacy, privacy frameworks, the role of nurses, electronic health records, patient information breaches in general and breaches involving nurses.

The environment surrounding information acquisition, storage, retrieval, transmission, and use is one marked with complexity and sometimes, even confusion. This environment is constantly changing with time and has often been described as a moving target. Two components, technology and ethical-legal aspects of the patient information environment are noteworthy due to the impact and implications they often have on privacy and security. The evolution, use, impact and implications of electronic health records are discussed in some detail.

Ethical guidelines and regulatory compliance are also be given considerable attention.

Nursing has been defined as an art and science (Leininger, 1984). In its art form, nurses use intuition, are expressive, subjective, creative, humanistic, and holistic. Their involvement in

the use and management of patient information whether implicit or explicit cannot be disputed. The purpose of the reviews mentioned above was to identify gaps in research and appropriately situate my research along the spectrum of work already done and those that are yet to be done.

2.2.1 Patient Information Privacy and Security

When it comes to the “language” of information privacy and security, the same expression may mean different things to different people. If people act on their own subjective interpretation of such expressions, the consequences could be devastating. In the sections that follow, attempts will be made to clarify some of the meanings given to terms and expressions from existing literature. The building blocks that constitute the meaning of patient information privacy and security would be laid out as well. Although reference is frequently made to “privacy and security” in this literature review and throughout the dissertation, attention will be focused on privacy considerations. In the context of my study, privacy is the “end” while security is the “means to the end”. In order to contain the study, only details of privacy considerations will be elaborated upon. Details of security considerations will be reserved for future research. The two terms, privacy and security are often used together perhaps as a persistent reminder that privacy is achieved through security. The two terminologies will be appropriately defined subsequently.

2.2.1.1 Patient Information: Introduction. In order to fully comprehend the nature and meaning of patient information, some understanding of the terminology used in association with patient information is necessary, including data, information, and knowledge. Key concepts and definitions of data, information and knowledge, and patient information will be addressed here.

2.2.1.2 Data, Information, and Knowledge. Data items refer to an elementary description of things, events, activities, and transactions that are recorded, classified, and stored but not

organized to convey any specific meaning (Rainer et al., 2011). Although data items are raw in nature and by themselves may not convey any specific meaning, when pieced together can be revealing. Data items should therefore be of importance when it comes to privacy and security.

Laudon and Laudon (2014) define information as data that have been shaped into a form that is meaningful and useful to human beings. This definition is not only important to understanding the distinction between data and information, but also foundational for gaining insight into some of the various mechanisms used to protect patient information, such as encryption.

Knowledge consists of data and/or information that have been organized and processed to convey understanding, experience, accumulated learning, and expertise as they apply to a current business problem (Rainer et al., 2011). Laudon and Laudon (2014) identify three kinds of knowledge that organizations must deal with. Knowledge that exist within the organization in the form of structured text documents (reports, etc.), semi-structured knowledge such as emails, voice mail, digital pictures, etc., and knowledge that resides in the heads of employees which they refer to as tacit knowledge. Regardless of how knowledge is acquired or exited in an organization, steps should be taken to ensure that this knowledge is properly managed and protected, particularly, if such knowledge pertain to patients and their privacy. During the discussions that follow and throughout the literature review, the terms data, information, and knowledge will be used interchangeably. Patient information is a specific form of information, and special in the sense that unlike other forms of information, it belongs to the category of information that require protection.

2.2.1.3 Patient Information. Following from the brief definitions and discussions above, patient information can be a wide collection involving data, information, and in some cases, even knowledge. A logical question to ask in a study that explores protection of patient information is, “what is being protected”? Buckovich et al. (1999) conducted a comparative review and analysis based on compilation of privacy, confidentiality, and security principles from many sources. According to these authors, an important finding was that seven of ten sources utilized the same words to describe information to be protected – information that makes individuals “identifiable” or “reasonably identifiable”. Samarati and Sweeney (1998) made reference to explicit identifiers of patients to include data such as name, address, and phone number. In their words, “.... there remains a common incorrect belief that if data looks anonymous, it is anonymous” (p. 2). They went on to say that data holders, including government agencies, often remove all explicit identifiers from a set of data so that other information in the data set can be shared. The authors believed that de-identifying data provides no guarantee of anonymity. They provided an example in which information in a city’s voters list was purchased and with data supposed to be anonymous, certain individuals were able to easily re-identify medical records. Their example should make data holders seriously rethink any attempts to categorize patient information for purposes of assigning levels of importance to data and how they are used in primary, secondary, or tertiary healthcare organizations.

Available literature does not seem to be clear on explicit classification of patient information for the purposes of defining levels of patient information sensitivity. Barrows and Clayton (1996), in their review of the conflicting goals of accessibility and security for electronic medical records defined sixty-eight medical records user types and six classes of data but do not

provide details of the classes of data. When describing data access control they appeared to be familiar with, the authors wrote that access to data on very important personalities (VIPs) and hospital employees invoked an additional screen message warning that all user activities are recorded. Their description suggested a form of data classification based on social standing, but lacks the necessary details to draw any valid conclusions from.

When it comes to protecting patient information, El-Emam et al. (2011) have suggested that the components of information, data, can be as important as the meaningful information itself. In the context of this study, personal health information will be synonymous with patient information.

2.3 Information Privacy and Developments

This section examines the meanings of privacy and patient information. Historical developments in privacy, are also briefly discussed.

2.3.1 *Privacy*

Many have alluded that defining privacy could be notoriously difficult because of its multidimensionality and broadness, and in some countries, the concept of privacy was not previously defined (Culnan & Williams, 2009; Smith, 1999; Tsai et al., 2010). Parks et al. (2011), using the definition of Westin (1967) have stated that privacy is the claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about them is communicated to others. According to Leino-Kilpi et al. (2001), the term privacy derives from two Latin words “privatus” and “privo”, which means “to deprive”. The CARNA (2014) defined privacy as the general right of the individual to be left alone, to be free from interference, from surveillance, from intrusion, and from interruption. Privacy also has to do with

an individual's right to determine what information about himself/herself may be collected, used, and disclosed. The patient's right is to determine when, how, and to what extent individuals want to share information about themselves with others. In another article titled "Privacy and management of health information standards", CARNA (2020b) reiterated the importance of privacy and management of health information standards to regulated members at all times, in every domain of practice. The article goes on to mention that, regardless of how a health service is paid for, the HIA applies to all health information collected, used, and disclosed by custodians in relation to that health service.

Leino-Kilpi et al. (2001) assert that privacy is a basic human need and recognized as one of the important concepts in nursing and health care ethics. As a member of a profession, it is the duty of the RN to report any malpractice witnessed or violation of patient rights. According to CNA's (2008, 2017) *Code of Ethics*, registered nurses recognize the importance of privacy and confidentiality and safeguard personal, family and community information obtained in the context of a professional relationship. While privacy is traditionally understood to be a state of social withdrawal, Palen and Dourish (2003), following the thinking of Altman (1975) believed that privacy is a dialectic and dynamic boundary regulation process. As a dialectic process, privacy regulation is conditioned by expectations and experiences, and by those of others with whom we interact. As a dynamic process, privacy is understood to be under continuous negotiation and management, with the boundary that distinguishes privacy and publicity refined according to circumstance. Here, people optimize their accessibility along a spectrum of "openness" and "closedness" depending on context.

Several forms and perspectives on privacy in general, and patient information privacy, specifically, have been described in the literature. Malin et al. (2013) cited the work of Dwork and Pottenger in 2013, in which they described the notion of differential privacy from a theoretical perspective. In their model of protection, researchers using a database containing patient information are permitted to ask queries of a database which subsequently responds with a perturbed aggregate response. According to them, this response is perturbed such that it is guaranteed that the researcher cannot determine whether a specific individual contributed to the database.

Altman (1977) proposed that privacy can be described either as an ideal, desired state or as an achieved end state. Drawing from Altman's (1977) perspective, Leino-Kilpi et al. (2001) concluded that if the desired privacy is equal to the achieved privacy, then there exists an optimum state of privacy. Such optimum privacy can be illusive in some cases. In the Canadian army, for example, health professionals, including civilian and military physicians may be forced to choose between obeying orders and upholding the values of their profession (Hebert et al., 2010). In their paper, they related that the duty to inform the patient as well as the process of explicitly defining the context of information access (who, why, when and how) of medical records also vary significantly from country to country. For instance, in the United Kingdom (UK), there are provisions for patients to learn who has had access to their personal health information and to request restrictions on use and disclosure. According to the authors, no such controls exist in the Canadian system.

Moore (1997) has suggested that privacy is like good art, you know it when you see it. This author suggested that from the point of view of ethical theory, privacy is a curious value.

While it seems to be something of very great importance and something vital to defend, privacy seems to be a matter of individual preference, culturally relative, and difficult to justify in general. Moore attempted to defend the importance of privacy using the age old philosophy on instrumental and intrinsic values. He defined instrumental values as those values which are good because they lead to something else which is good, and intrinsic values as those values which are good in themselves. He concluded that almost everyone would agree that privacy has instrumental value, offering protection against for example, the risk of discrimination, if a person's medical condition is publicly known. The intrinsic value perhaps derives from the satisfaction of knowing that personal information is protected from public knowledge.

Leino-Kilpi et al. (2001), claimed that many studies have employed Altman's (1977) concept of privacy, emphasizing the aspect of control. The authors pointed out that in health care, control of knowledge is an important part of privacy. They added that control includes the decisions as to what information is given to others, what is not, and what information is shared with others.

There are yet other perspectives regarding privacy such as one held by Chalmers and Muir (2003). They believed that privacy is not an absolute right, as suggested by others and has to be balanced against counterclaims such as the right of others or societal group. Striking the balance between individual and societal rights could be challenging. The authors wrote that the question of having to seek explicit consent always from patients for any use of data apart from direct clinical care was considered and rejected by the Confidentiality and Security Advisory Group for Scotland. This should provide a glimpse of the state of affairs in the healthcare

industry when it comes to the privacy and confidentiality of patient information. There appears to be dissenting schools of thought in this area.

The concept of privacy has become so information enriched that “privacy” in contemporary use typically refers to informational privacy, though of course, other aspects of the concept remain important (Moore, 1997). However, there is a sense in which information privacy has been defined as more than “informational self-determination” protected by formal notice and consent, and introducing a substantive notion of privacy rooted in consumer expectations (Bamberger & Mulligan, 2010). Bamberger and Mulligan elaborated that the identification of privacy with consumer expectations as reflected in malleable context-dependent norms, moreover, has moved privacy from a compliance-oriented activity to a risk-assessment process, requiring firms to embed privacy in decisions about product design and market entry, as well as policy development. In their opinion, the success of privacy protection, then, would be measured not by the vindication of notice and consent rights, but in the actual prevention of substantive harms, such as preventing data breaches, or treating information in a way that protects the "trust" of those whose information is at stake. This trust is often achieved through maintaining confidentiality.

The word “confidentiality” is often used in conjunction with privacy. The CNA (2008, 2017) has defined confidentiality generally as the duty of someone who has received confidential information in trust to protect that information and disclose it to others only in accordance with permissions, rules or laws authorizing its disclosure. The healthcare provider and patient relationship is characterized by intimacy and trust, and confidentiality is embedded at least implicitly in patient-provider interactions (Barrows & Clayton, 1996).

Regarding who owns patient information, Barrows and Clayton (1996) believed that data ownership is a legally complex issue and ownership of a medical record is at best a limited right that is primarily custodial in nature, and information contained in the record is often characterized as the patient's property. Barrows and Clayton also expressed their opinion of privacy this way; “.... privacy is partly in the eye of the beholder, and an intrusion of privacy perceived by one person may be considered as convenience by others (targeted marketing, solicitation by insurers, etc.)” (p. 142).

While most academics look for the core meaning/essence of privacy, others emphasize the multifaceted dimension of this concept, which has led some academics to even claim that it is irrelevant to define privacy since such definition bears the risk of limiting and “freezing” its meaning and effect (Uppsala University, 2012). The authors also assert that privacy is a disputed concept and has several criticisms. Among its many criticisms are the claims that it is a form of individualism that neglects the common good. Nissenbaum (2010) mentioned another relatively new development in privacy theory, which is the assumption that privacy is not an absolute value but a form of contextual integrity. Thus, if privacy should be protected or not depends on the situation, the type of information, and the subject or group. The perception people have concerning patient data ownership could perhaps influence attitudes towards privacy and how it is managed by health organizations.

2.3.1.1 Managing Information Privacy. Patient information privacy management makes for a delicate balancing act. This dichotomy was expressed by Cavoukian and Rossos (2009), in that while patient information privacy is extremely sensitive, requiring the strongest privacy and security protections to prevent unauthorized use and disclosure, it must as well be readily

available to the broad range of healthcare providers. Parks et al. (2011), citing the works of Fernando and Dawson, 2009; Mohan and Razali Raja Yaacob, 2004; and Croll, 2010, who have pointed out that in the presence of increasing penalties for non-compliance and privacy operational challenges, organizations are facing challenges on how to respond appropriately to privacy threats while not impeding health care workflows. Personally identifiable information and protected health information are some of the most portable targets for cyberattacks (Forrester Research, 2013). The health industry was the most targeted, accounting for 43% of breaches (ForgeRock, 2020). Although this is in reference to the United States, the trend may not be different for Canada. In an article published by the CBC (2020a) and titled “Hospitals ‘overwhelmed’ by cyberattacks fueled by a booming black market”, some experts call for national standards and federal money in the battle against healthcare data security breaches.

In order to indicate the seriousness of cybercrime with regards to patient information, the author indicated that Canada's health system is under siege from unrelenting cybercriminals.

These criminals are trying to access patient information and other data that could be subsequently, in some cases used to hold the affected individuals or institutions for ransom. The CBC (2020b) goes on to comment that healthcare professionals and cybersecurity experts say that hospitals and clinics are unable to cope with the growing threats.

The diverse perspectives on information privacy discussed above should not suggest that management of information privacy and security be an overly complicated matter. According to Forrester Research (2013), keeping information private is a continuous process. Important to understand is that privacy protection, which can often seem abstract and inconsistent, consists of identifiable information assets, repeatable processes, and specific security controls. A strong

privacy program can help reduce the uncertainty of compliance and the number of privacy abuses, security incidents, remediation costs, fines, and damage to reputation.

Palen and Dourish (2003) have described three privacy boundaries which they believed characterized the management of privacy. They made reference to the disclosure boundary, which they described as where privacy and publicity are in tension. At this boundary, determinations are made about what information might be disclosed under what circumstances, with varying degrees of direct control. The second boundary is where the display and maintenance of the identity of parties on both sides of the information exchange occurs. They referred to the third boundary as temporality and associated this boundary with time, that is, where past, present and future interpretations of and actions upon disclosed information are in tension. Effective management of privacy means clearly understanding and interpreting these boundaries in the context of the organization. Only then could appropriate actions be taken to minimize the effects of privacy breaches.

In their classification of information privacy research issues, Parks et al. (2011) mentioned three areas of importance; information privacy threats, information privacy responses, and influencing factors. These areas could be significant in effectively managing information privacy. In their scheme, information privacy threats included data collection, data disclosure, unauthorized access, secondary use, and errors (Parks et al., 2011). Information privacy responses had two components, human and technical. According to the authors, mitigating identified threats takes education and training of people. Another human aspect they mentioned was building a culture of privacy within the organization (Parks et al., 2011). Technical responses to privacy included the use of policies and technologies. In order to ascertain if

responses are working, Parks et al. (2011) suggested a privacy impact assessment. Influencing factors are often external to the organization and consist of institutional, competitive, moral/ethical, and fair information practices (FIPs). The organization needs to be aware of and respond appropriately to privacy regulatory mandate, fulfil its moral or ethical obligations which often translates to having good business practices, and follow information processing standards in order to thrive (Parks et al., 2011). Opinions and perceptions regarding several aspects of privacy of personal information vary.

2.3.2 Privacy Perceptions

Opinions about how people perceive and feel about patient information privacy differ among countries and even within different regions of a country, with generally low levels of trust and confidence in the prevailing patient information privacy environment. Ball et al. (2007) have reported a study conducted in the U.S in which two-thirds of American consumers expressed serious concerns about the privacy of their personal health information, and 52% of all consumers were concerned that information they provided to an insurer on claims might be seen by an employer and used to limit job opportunities. They pointed out that this was an increase from 1999 when only 36% expressed similar concerns. Concerns expressed by consumers then, have not abated even in recent times. An article published by the New York Times (NYT, 2019) indicated the push by Google to store and analyze the data of millions of patients in an effort to improve medical services. One could appreciate the public outrage and escalation of concern. It is interesting to note that as of this writing, Google has partnered with Ascension, a U.S medical organization that operates 150 hospitals in 20 states. The implication for such partnership is that the data of hospital patients could eventually be uploaded to Google cloud computing platforms.

The article indicated that it is legal for health systems to share patients' medical information with business partners like electronic medical record companies (NYT, 2019). Many patients may not trust Google with their personal medical details. Mention was also made of the fact that Google has already paid multiple fines for violating privacy laws (NYT, 2019). Such concerns have prompted several reformations regarding protection of personal information in the insurance industry.

The National Law Review (2020) has published an article that describes what the United States government is doing in some parts of the country to ensure the security of sensitive personal information in the hands of insurance organizations, for example, the California Consumer Privacy Act of 2018 has been enacted to protect personal information. The authors add that those most concerned about misuse of personal health information were racial and ethnic minorities. They also reported a grim reality where one in eight consumers had asked a physician not to record a problem, chose to go to another physician to avoid telling their regular doctor about a condition, and other self-protection behaviours as a result of privacy concerns.

Stone et al. (2005) cited a project undertaken by the NHS Information Authority in conjunction with the Consumers' Association in the UK that found that people generally wanted data to be anonymized when used other than for treatment, unless consent was sought. They also mentioned a study from the Netherlands by Schers et al. (2009) which found that not all patients were happy for their medical record to be shared fully with an on-call general practitioner or practice assistant. In the UK, 10% of patients who were prepared to complete a questionnaire as part of a research project withheld permission for researchers to review their general practice records. In the U.S, a 1996 privacy survey cited by Anderson (2000) reported that 18% of the

public felt that the use of patient records for medical research without the patient's explicit permission was inappropriate, and even worse, 75% of respondents felt that the use of prescription data to detect fraud was unacceptable.

The results of a similar study conducted by EKOS Research Associates in 2007 on behalf of Canada Health Infoway (CHI), Health Canada, painted a rather encouraging picture regarding how Canadians perceived safety and security of health information CHI, Health Canada [HC], & Office of the Privacy Commissioner [OPC] of Canada, 2007). According to the study, two in five Canadians (39%) believed that the health information that existed about them was "safe and secure" (5 to 7 on a 7-point scale) and an additional 40% said that the information was at least "moderately safe and secure". On the other end of the spectrum, there was less than one in five (17%) that worried that the information was "not safe and secure" (1 to 3 on a 7-point scale). With the exception of a few more Canadians preferring to indicate that health information was "moderately safe and secure" as opposed to just "safe and secure", these results were virtually unchanged from 2004. Furthermore, perceptions of the security of health information varied across the country, with residents of AB (46%) and Atlantic Canada (44%) the most likely to consider the information "safe and secure". The report added that the perceived safety of health information also declines rapidly with age (60% of youth consider their health information "safe and secure" compared to 34% of seniors) (CHI, HC, & OPC, 2007).

The OPC of Canada (2019), conducted a survey of Canadians on privacy. The main objective of the research was to explore Canadian's awareness, understanding and perceptions of privacy-related issues. Results of the survey shed light in many areas of privacy in Canada. These areas included general knowledge of privacy, general knowledge of how to protect privacy

rights, concern about protection of personal privacy, knowledge of how new technologies affect privacy, views on whether businesses respect rights, views on whether the federal government respects privacy rights, impact of privacy breaches on willingness to share personal information, and many other areas (OPC, 2019).

The highlights of the results of the OPC (2019) survey were the following: Canadians feel they are knowledgeable about their privacy rights but are still concerned about privacy protection; Canadians are concerned about how their online information will be used and take security measures to protect their personal information; Canadians are also concerned about the collection and use of information from their body for non-medical reasons; Canadians' willingness to do business with a company would be affected by the introduction of financial penalties for the misuse of personal information and by a company's privacy practices; news stories on security breaches still have a large impact on Canadians' willingness to share personal information (OPC, 2019). This is reflected, in part, in the steps taken by Canadians to protect personal information; Canadians lack a clear understanding of the Government of Canada's collection of personal information about citizens.

Despite limited knowledge, most Canadians would be at least somewhat comfortable with the Government of Canada sharing their personal information with another federal department with their consent; Canadians feel they lack control over how their personal information is being used and want government to be responsible for helping them to protect their personal information (OPC, 2019).

When asked about trust in those with access to health information, Canadians continued to express a high degree of trust in health care professionals to preserve the safety and security of

their personal health information. On the issue of trust, the report stated that by a wide margin, doctors were still the most trusted, with just about half of all respondents (46%) saying they have “great deal of trust” in these individuals (a 7 on a 7-point scale). Other frontline caregivers also scored extremely well, with about one in four affording nurses (25%), pharmacists (25%), and administrators in family doctor’s offices (22%) the highest trust scores. Health care providers in hospitals scored slightly lower (16% “a great deal of trust”), but they were still highly trusted overall. For all of these professionals, there was at least an additional 40% that assigned high trust (a score of 5 or 6 on the same scale), while fewer than one in ten typically assigned low trust (a score of 1 to 3) (CHI, HC, & OPC, 2007).

Important to note is that the measures used here are based on perception and not reality. The studies mentioned above did not provide the basis of the recorded perceptions. Therefore, it is important to not jump to quick conclusions based on the results reported. Such quick conclusions not based on empirical data can breed a false sense of security and possibly lead to some sort of complacency when it comes to health record privacy and security.

Five years later, the 2013 version of the same research survey on privacy-related issues published results that do not show remarkable differences from the 2007 study. The 2013 report indicated that in general, there has been no change or movement over the past five years when it comes to Canadians’ level of concern about the safety and security of their personal health information (OPC, 2013). Most believe such information is at least moderately safe (82% in 2012 vs. 79% in 2007), but less than a majority are willing to say it is definitely safe and secure (41% in 2012 vs. 39% in 2007). The results of the survey however suggested that public trust in health care professionals to safe-keep their personal health information may be softening, adding

that it is unclear whether this softening can be specifically linked to the usage of electronic health records. There was no evidence in the survey that suggested that the small declines between 2007 and 2012 reflected anything other than a slight decline in trust in health care professionals in general (OPC 2013).

The OPC (2013) research made reference to data from other survey research on privacy-related issues conducted in Ontario that showed a dip in the public's confidence in the health care system and professionals in general over the last several years but did not mention the reason for the decline in confidence. According to the researchers, a large majority (85%) of Canadians believed that people withhold health-related information from their doctor. The assumption is that this happens most often because people are embarrassed to tell their doctor and not because of specific privacy concerns. This behavior could be interpreted as privacy from their doctor and thus constitutes a concern that may warrant further investigation. A patient protectionist behavior is what could prevent the patient from receiving the needed medical attention. In the report, the majority of Canadians did not believe that people would be any more likely to withhold health information from their doctor if it was going into their EHR (60% indicated it would make no difference –or- would make people less likely) (OPC, 2013).

Established in 1983, the Office of the Privacy Commissioner of Canada (OPC) acts as Canada's privacy guardian (OPC, 2011). The OPC's mandate is to ensure that organizations entrusted with personal information are in compliance with federal privacy laws. In 2011, the OPC commissioned Harris/Decima to undertake a survey of Canadians to gauge understanding and awareness of privacy issues, legislation and federal privacy institutions, particularly in each of four priority areas: information technology and privacy; national security and privacy;

identity integrity and protection; and genetic privacy. Similar studies had been conducted each year for the period between 2006 and 2009. The study reported that 30 percent of Canadians were aware of a federal institution that helps them with privacy and protection of personal information from inappropriate collection, use, and disclosure. Most felt that their knowledge of personal privacy rights under the laws protecting their personal information was poor. In this study, Canadians generally felt that they were doing a good job at protecting their privacy. Canadians wanted government organizations and businesses to face consequences for breaking privacy laws. Although the importance of privacy protection was obvious in the study, many felt it was not an issue they had control over. The study also found that privacy concerns related to the internet, computers, public wi-fi, and social networking were on the rise (OPC, 2011). This concern may be partly due to perceptions about accessibility to information.

2.3.3 Patient Information Accessibility

Patient information exists primarily in two forms, paper records and electronic records. The popularity of electronic records and variations thereof is increasing. Literature on the thoughts, beliefs, and practices concerning how paper and electronic records should be kept, accessed, and used suggests that there is no consensus among clinicians and holders of patient information on how best to handle patient information collection, storage, transmission, and use. This section of my literature review looks at paper and electronic patient information, their accessibility (recording, retrieving, listening and viewing), the supply and demand for this information, their uses, and the dynamics not only of information exchange, but the environment surrounding it as well. Privacy and security implications will also be briefly discussed.

Traditionally, patient records have been kept on paper and stored in cabinets at different locations in a clinic or hospital. While waiting at a reception area, it is not uncommon to see patient records stored in what appears to be mailboxes, for convenience and easy access. It is also common knowledge that such methods of record keeping are used in primary, secondary, and tertiary care. Patient information is typically directly recorded by clinicians. Hayrinen et al. (2007) found that data were recorded in electronic health records (EHRs) by different groups of health care professionals, adding that secretarial staff recorded data from dictation or nurses' or physicians' manual notes, and that some information was also recorded by patients themselves and validated by physicians.

Research and development are ongoing in several countries around the world to develop an infrastructure for national health information; examples include Canada, Australia, England, the United States, and Finland (Hayrinen et al., 2007). The authors did not mention how the infrastructure is going to be accomplished, but the most logical approach would be through electronic databases. The push towards electronic patient records is unprecedented. Hayrinen et al. (2007) commented that besides national projects, the European Union launched the European eHealth Action Plan in 2004. Details on electronic health records and their variations will be provided subsequently under the relevant sections in this review.

The terminology used in the literature in relation to access to patient information can be confusing. For example, “access by authorized users” could be mistaken to mean an open access to clinicians. In many cases, access needs to be on an “as needed” basis. For example, the fact that Nurse A is working in the same ward as Nurse B does not mean they could freely exchange information about the patients assigned to each of them, even with authorization to access all

patient information. However, if they have to cover for each other during breaks – they certainly do need to share any pertinent information; in addition, if there is pertinent information about the patient, it should be shared, as the nurse may have that patient in the next few shifts.

Malin et al. (2013) divided patient information accessibility and use into zones that could provide clues for strategic management of privacy protection. The first zone corresponds to the point at which health information is collected from patients, which they call the collection zone.

According to them, the collection may occur while an individual is physically located at a healthcare provider or beyond, such as through a website, or an application running on a mobile device. In their estimation, privacy in this zone tends to be concerned with who can collect health information, how much information should be collected, at what time, and for what purpose, with anonymity being a key consideration in this zone.

They referred to their second zone as the primary use zone which corresponds to the context in which the data have left the control of the patient and are housed in a system controlled, or accessed by those who provide primary service such as provision of care or for a specific research. They believed that in this zone, privacy tended to be realized through what they call confidentiality (who is permitted to access or use the data and for what purposes) and security (ensuring that the data is protected at rest or in transit between authorized entities). Their third and final zone corresponds to the scenario in which data are utilized for purposes different from their primary use. They have labeled this zone the secondary use zone. Here, data may be used by the organization that initially collected the data or disseminated to external entities. They claimed that privacy issues that tend to arise here pertain to anonymity and consent.

The zones described by Malin et al. (2013) above provide a reasonable platform for following the patient data path. Zones may also be useful for conducting investigative study of the threats and vulnerabilities of the data at their “transient homes”. This classification could be used to do targeted risk assessment of the “data residence”, and subsequently for prescribing appropriate risk mitigating and threat reducing safeguards for patient information to ensure privacy and protection.

There are several propositions regarding patient information availability and control. One of the earlier ideas was championed by Mandl et al. (2001) that proposed two doctrines. The first one was to guide the development of electronic medical record systems that would be designed in a way to allow exchange of all their stored data according to public standards. The second doctrine was based on the premise that patients should have control over access and permissions. They further added that because an individual may have different preferences about different aspects of his or her medical history, access to various parts of the record should be authorized independently, for example, psychiatric notes may deserve closer protection than immunization. Initiatives in the proposed direction seem to be in their infancy, and the literature is not exactly clear on what is meant by a patient’s control of his or her medical records other than deciding who gets their information and who does not.

Situations leading to request for access to patient medical records include a routine doctor’s visit, emergencies, request from place of care such as home, and even when a patient is incapable of consent. In some of these situations, the speed of access to pertinent information could mean the difference between life and death, in which case ready access to needed information may supersede due diligence with respect to privacy. In England, a study conducted

by Stone et al. (2005) reported that data sharing with employers and insurance companies were seen as potential problem areas, particularly by staff but also by some patients. More practical concerns were also raised, such as the visibility of information on computer screens and the difficulty of maintaining confidentiality in a busy waiting room. According to the authors, this is what one practice nurse had to say; “My screen’s directly opposite the hatch and so people can quite easily look straight in and see who is on Viagra down the road” (Stone et al., 2005, p. 786). Such matters that often have simple fixes could be good indicators of bigger problems within a system. Therefore, it was not surprising to me when the authors wrote in their discussion that staff interviews they conducted suggested a limited awareness of the issues involved and the lack of clear relevant policies in general practices.

Access to and sharing of patient information also comes by way of electronic mail. Kane and Sands (1998) define patient-provider electronic mail as computer-based communication between clinicians and patients within a contractual relationship in which the health care provider has taken on an explicit measure of responsibility for the client’s care. In their paper entitled “*Guidelines for the Clinical Use of Electronic Mail with Patients*”, they clarified that their guideline did not address communication between providers and consumers in which no contractual relationship existed, as in an online discussion group in a public support forum. What the authors failed to mention in their definition was whether the contract they refer to in their definition is a psychological contract or a written one. There is a significant difference between the two. Psychological contracts are often implied and unwritten and as such of little legal consequence. Several forms of email also exist, further complicating the electronic patient record environment.

2.3.4 Historical Developments in Information Privacy

The notion of privacy in the healthcare domain is at least as old as the ancient Greeks and the necessity of patient privacy was recognized as a core principle, or even a right, that must be upheld (Malin et al., 2013). Protection of privacy in Canada has been in existence well beyond the establishment of privacy governing institutions. For example, the Office of the Privacy Commissioner (OPC, 2011) was established about 32 years ago but privacy concerns for income tax, financial transactions, and medical records were important prior to OPC's existence.

In his paper entitled “Social and Political Dimensions of Privacy”, Westin (2003) provided contemporary stages of privacy development. After describing what he called a privacy baseline, which covered the period between 1945 and 1960, he advanced three phases of contemporary privacy development: 1961–1978, 1980–1989, and 1990–2002. Within each period, he described changes in three factors that drove privacy development. The three factors were, new technologies and their applications by organizations, social climate and public attitudes, and organizational policies and law.

Westin’s (2003) view of the 15 years following the end of World War II was a period (1945–1960) of limited information technology developments, marked by high public trust in government, business, and non-profit sector. According to him, the general public had a level of comfort with information collection and use activities. Other defining characteristics of this period were that the law addressed privacy issues in traditional legal concepts and accepted business-marketing and employer uses of personal information as not violating any personal legal right (Westin, 2003). In the first era of contemporary privacy development (1961–1979), information privacy was explicitly seen as a social, political, and legal issue of the high-

technology age. The social climate was one of civil rights struggles and other social protest movements. Concerns over privacy in this new social order developed. Several advances in physical, psychological, and data surveillance technologies were made and used. Third-generation mainframe computer systems were becoming available. Organizations and individuals began to recognize the down side of technology and privacy. There were calls for new privacy standards and protective actions during this era, which subsequently led several countries to start investigating the nature, dynamics, and impact of technology applications and to explore ways to apply privacy balances. In the U.S. context, the Fair Information Practices (FIP) framework which combined privacy standards with due process, consumer rights, and equality was formulated (Weston, 2003).

The second era of privacy development, which was the period between 1980 and 1989 was one of enhanced computer and telecommunications but without fundamental changes in information-society relationships bearing on privacy (Westin, 2003). Computers were however not connected to the larger world and thus did not affect the privacy situation. The public was becoming apprehensive about combining information resources of separate industries. Although there was warm appreciation of the benefits and conveniences of new technologies, there were worries about the potential misuse and abuse. In the U.S., several federal legislation, such as the Privacy Protection Act of 1980 came into existence. Privacy became important as a political issue. Westin (2003) remarked that while the U.S. committed to FIP, and sector-based regulatory approach, European nations used national data protection laws that covered the entire governmental and private sectors, using independent national data protection agencies in the early 1970s. Important to note is that adoption of privacy guidelines or laws from one region of

the world to another was not uncommon. For example, the U.S. adopted the privacy guidelines of the Organization for the Economic Cooperation and Development in 1980, and by the early 1990s, were written into formal employee or consumer privacy policies of about 200 American companies (Weston, 2003).

The third era of privacy development in Westin's (2003) scheme was that between 1990 and 2002. According to Westin, privacy became a top priority social and political issue globally and impacted by the September 11, 2001 terrorist attack. Weston (2003) pointed to five major developments in technology that framed the privacy debates, these were: the rise of the internet in the mid-1990s with high levels of self-disclosure by internet users; the now ubiquitous wireless communication devices including the cell phone affording instant mobility and convenience; the human genome that had the promise for use in family planning and health care; development of data mining software and automation of government public record systems making it possible to produce in-depth consumer profiles and, fostering personal target marketing; and, law enforcement concerns that encryption could immunize illicit online communications.

The general concerns raised around the technological developments mentioned above in relation to privacy were that web sites could track visitors and document their usage. Wireless communication devices allowed location of individual users and the possibility of sending them unsolicited marketing messages. The advent of the human genome meant that genetic tests might be required for determining access to health or life insurance or employment (Westin 2003). Setting privacy rules for genetic information was a monumental task. Identity theft was a big issue as a result of large amounts of personal information in government and business record

systems. Efforts to limit encryption, particularly in the U.S. attracted a lot of technology industry and civil libertarian challenges. Westin (2003) offers a detailed narration. His account of developments in privacy, in a broader sense appears to be congruent with events taking place in Canada.

During the third annual *Access to Information, Privacy and Security Congress*, Stoddart (2012) briefly recounted some historical perspectives in the area of privacy in Canada. According to her account, the year 1982 marked a leap forward for privacy rights in Canada, with parliament enacting the Privacy Act. There was little by way of technological advancement. As she put it, “the 1980s were also simpler times for privacy”. Around the mid-1980s, concerns about more complex privacy issues such as data matching, cross border information flows, smart cards, and genetics began to surface.

The period from 1992 to 2002 saw rapid changes such as more powerful computer technology, advanced software sophistication, and transformation of personal information into commodity.

Along with these changes came greater risk for privacy. There was greater awareness of the capability of new technologies to collect, analyze, and store personal information in ways unimaginable in the typewriter era. Park et al. (2011) believed that early 1990s might be considered as a starting point of information privacy research in management information systems. The third decade following the period 1992 to 2002 was marked by two main developments that occurred at the end of the second decade and impacted the third (Stoddart, 2012). There was the extension of the OPC of Canada’s (2011) mandate with the passage of federal private-sector privacy legislation, the *Personal Information Protection and Electronic Document Act* (PIPEDA). The second event that affected how Canada and the Western world

view privacy and security was the terrorist attack on September 11, 2001. Many nations responded with a number of security initiatives including collection, analysis, and cross matching of personal information. The anti-terrorism act introduced during the period which necessitated broad surveillance of organizations and individuals meant that steps should also be taken to ensure that privacy rights were not unduly eroded. Privacy concerns related to air travel and “lawful access” concerns have also been addressed.

Stoddart (2012) commented that Canadians need to be protected by modern, effective privacy laws, adding that at the moment, Canada is lagging in this regard. She reiterated the need to strengthen the privacy laws in the light of modern information technologies, evolving government practices, and the expectations of Canadians. She also noted three trends and discussed in some detail the nature of these trends: the rise of what she called “multinational online powerhouses” which play a central role in our day-to-day online activities; the extent of surveillance by the U.S National Security Agency and similar bodies in other countries; and individual responsibility in an online world where anybody can say anything about anyone to everyone. Stoddart (2012) pointed out the inadequacy of existing privacy frameworks to address the new challenges.

2.3.5 Privacy Frameworks

Information flow as well as its protection is important to businesses and government organizations. In order to strike a balance between information accessibility and protection, several privacy frameworks have been proposed and placed in operation in different parts of the world. Privacy frameworks may be used as tools to help think about and frame discussions about privacy, and understand privacy requirements (Organization for Economic Co-operation and

Development [OECD], 2010). Frameworks commonly referenced in the literature include the OECD Privacy Principles, Asia-Pacific Economic Cooperation (APEC) Privacy Principles, Fair Information Privacy Principles, Government Privacy Principles, and International Standards Organization (ISO) Security Principles. A number of privacy and security laws, regulations, policies, and procedures in operation today may have their roots in one or more of the frameworks mentioned above. This section summarizes key privacy frameworks.

2.3.5.1 Organization for Economic Co-operation and Development (OECD) privacy principles. The OECD privacy principles provide the most commonly used privacy framework internationally (OECD, 2010). This framework is closely related to the European Union member nation's data protection legislation and cultural expectations. The OECD privacy principles are part of the OECD guidelines on the protection of privacy and trans-border flows of personal data that was developed in the late 1970s and adopted in 1980. OECD provides a setting where governments compare policy experiences, seek answers to common problems, identify good practice and coordinate domestic and international policies. The OECD (2010) espouses eight privacy principles:

The first is the collection limitation principle which stipulates that there should be limits to the collection of personal data and data should be obtained by lawful and fair means, and where appropriate, with the consent of the data subject. This principle appears to be present in many regulatory compliance mandates around the world (OECD, 2010).

The second principle addresses data quality. The principle requires that personal data should be relevant to the purpose for which they are to be used and to the extent necessary for the purposes. Data collected must be accurate, complete, and kept up to date (OECD, 2010).

The third principle, the purpose specification principle states that the purposes for which personal data are collected should be specified not later than at the time of data collection. Also, use of the data be limited to the fulfilment of intended purposes. In the case the data are used for other purposes, such change in purpose needs to be explicitly stated (OECD, 2010).

Regarding the fourth principle, the use limitation principle, the OECD discourages the disclosure of personal data and adds that such data should not be made available for purposes other than specified, except with the consent of the data subject, or by the authority of law. The fifth privacy principle requires that personal data be protected by reasonable security safeguards against risks. Such risks include loss or unauthorized access, destruction, use, modification, or disclosure of data (OECD, 2010).

The openness principle, the sixth principle requires that there is a general policy of openness about developments, practices, and policies with respect to personal data. This principle advocates for a way of readily ascertaining the existence and nature of personal data, and why they are being used. The identity and usual residence of the data controller are also important components of this principle (OECD, 2010).

The seventh principle has to do with the rights of individual participants. This principle states that an individual should have the right to inquire whether or not data are being kept about them. Individuals should be informed what data are being kept about them within a reasonable time period, if necessary, at a reasonable charge, in a reasonable manner, and in a form that is reasonably intelligible. The individual participation principle allows individuals to be given reasons regarding denial of request and to challenge such denial. An individual can challenge for data about them to be erased, rectified, completed or amended (OECD, 2010).

The final (the eighth) OECD (2010) privacy principle is the accountability principle. The accountability principle calls for the data controller to be accountable for complying with measures that give effect to the principles above. Another privacy framework that has wide use is the APEC framework. The APEC framework briefly is described next.

2.3.5.2 Asia-Pacific Economic Cooperation (APEC) privacy framework. The APEC privacy framework was designed to enable regional data transfer to benefit consumers, businesses, and governments (APEC Secretariat, 2005). The framework recognizes the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region. Like the OECD (2010) privacy framework, APEC is a principle-based framework. According to APEC Secretariat (2005), this framework aims at promoting electronic commerce throughout the Asia-Pacific region. The APEC is consistent with the core values of OECD's 1980 guidelines on protection of privacy and trans-border flows of personal data. The APEC Secretariat stated that the framework reaffirms the value of privacy to individuals and to the information society.

The APEC privacy framework (APEC Secretariat, 2005) was based on the recognition of the importance of several issues. First, it was based on developing appropriate privacy protections for personal information with emphasis on minimizing the harmful consequences of unwanted intrusions and the misuse of personal information. The framework recognizes that the free flow of information is important for both developed and developing economies. The framework was developed to afford uniform approaches to data collection, access, use, or process. Another goal of the framework is to enable enforcement agencies to fulfil their mandate to protect information privacy. Lastly, the framework is intended to advance international

mechanisms for ensuring enforcement, and continuity of information flows (APEC Secretariat, 2005). The nine core principles of the APEC that make up the framework are briefly summarized below:

The first, is preventing harm principle. This principle recognizes the prevention of the misuse of personal information and consequent harm to individuals. This principle encourages the use of self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms for achieving prevention (APEC Secretariat, 2005).

The notice privacy principle aims at ensuring that individuals are able to know what information is collected about them and for what purpose it is to be used. The types of persons and organizations personal information may be disclosed to, are important elements of this principle. Also important are the identity and location of personal information controller. Personal information controllers are required by this principle to provide choices and means by which individuals can limit the use and disclosure of, and for accessing and correcting their personal information (APEC Secretariat, 2005).

Collection limitation principle limits information collected to that which is relevant to the purpose of collection. Collection must be lawful and by fair means, and where appropriate, with notice to, or consent of the individual concerned. The principle also recognizes that there are circumstances where providing notice to or obtaining consent of individuals will be inappropriate (APEC Secretariat, 2005).

The use principle stipulates that personal information collected should be used only to fulfil the purposes of collection and other compatible or other related purposes except with consent of the individual or personal information is collected, when necessary, to provide service

of product requested by the individual. Another exception is by authority of the law or other legal instruments (APEC Secretariat, 2005).

There is also the choice principle which says that where appropriate, individuals should be provided with clear, prominent, and easily understandable, accessible, and affordable mechanisms to exercise choice in relation to the collection, use, and disclosure of their personal information (APEC Secretariat, 2005).

The next principle has to do with integrity of personal information. Here, personal information should be accurate, complete, and up-to-date to the extent necessary for the purposes of use. The security safeguard principle makes it obligatory for personal information controllers to protect personal information that they hold with appropriate safeguards against risks (APEC Secretariat, 2005).

The eighth principle is the access and correction principle. Under this principle, individuals should be able to obtain confirmation of whether or not their personal information is held by a controller. Individuals could also have their personal information communicated to them in a reasonable time, at reasonable cost, in a reasonable manner, and in a form that is reasonably understandable. This principle allows individuals to challenge information about them (APEC Secretariat, 2005).

The final principle, accountability, requires that a personal information controller be accountable for complying with measures that give effect to the APEC principles. When transferring information, controllers should ensure that the recipient will protect the information consistently with the principles when not obtaining consent (APEC Secretariat, 2005).

2.3.5.3 Fair Information Framework. The fair information framework are a set of principles and practices that describe how information-based society may approach information handling, storage, management, and flows with a view toward maintaining fairness, privacy, and security in a rapidly evolving global technology environment (Gellman, 2015). The fair information practices have been in existence since 1973.

Gellman (2015) notes that there are fundamental beliefs upon which the fair information principles are based. First, there must not be personal-data record-keeping systems whose very existence is secret. Secondly, there must be a way for an individual to find out what information about him or her, is in a record, and how it is used. Provisions should be made for an individual to prevent information obtained from him or her for one purpose from being used or made available for other purposes without consent. Also, there must be a way for an individual to correct or amend a record of identifiable information about him or her. Lastly, any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data. The specific details of the principles are almost identical to that of the OECD (2010) privacy framework.

2.3.5.4 International Standards Organization (ISO). The ISO (2013) is a global standards body that develops and coordinates a vast range of technical standards. The main sub-committee within ISO responsible for numerous information technology security standards is the “SC 27”.

SC 27 in turn has several working groups in specific areas in information security. These working group areas include information security management systems; cryptography and security mechanisms; security evaluation, testing and specification; security controls and

services; and identity management and privacy technologies. The ISO framework covers a broad area in information security. Details of the ISO framework are well documented (ISO, 2013).

There are relationships among what appears to be disparate privacy frameworks. For example, the OECD (2010) privacy principles derive from the fundamental principles put forward by the advisory committee from the U.S. Department of Health, Education, and Welfare (HEW). The similarities and overlap among the various privacy frameworks could be described as remarkable. They all appear to seek to protect individual personal information and preserve human dignity. In some cases, however, the motivation has been to promote economic activity.

Some differences also exist between the different frameworks. For example, the APEC framework concentrates on actual or potential harm as a result of disclosing information, rather than the individual's rights pertaining to their information, as in the OECD principles. Important to note also is that while the OECD (2010) privacy principles have support among the European Union and other government legal regimes, the APEC framework is not supported by law.

2.3.6 Ethical-legal Environment of Privacy

In their “The Privacy and Security” research paper series, Uppsala University (2012), in collaboration with other academic institutions and agencies claimed that the legal conceptualization of privacy has emerged quite recently (the nineteenth century) and pointed to the work of Warren and Brandeis (1890), who strongly called for the recognition and protection of the right to privacy, and popularized the legal concept of privacy. Malin et al. (2013) also portrayed privacy as a societal phenomenon and added that the extent to which it is realized is dependent on how society chooses to codify the concept in policy and law. In line with this thinking, many provinces in Canada have enacted laws that indicate their commitment to the

protection of its citizen's health information. A good working knowledge of applicable regulations that affect privacy is critical, particularly for work environments that have the tendency to be litigious. Even though there are a multitude of regulations that address privacy, they all have common features.

The consumer-oriented understanding of privacy presented earlier in this literature review has given rise to laws in some countries that protect the interest of the consumer. In the U.S. for example, passage of the state security breach notification (SBN) laws is a means for binding corporate performance on privacy to "reputation capital". The legal ramifications of the laws have led to a number of non-legal phenomena critical to formation and spread of the legal notion of privacy compliance as consumer harm prevention. According to Bamberger and Mulligan (2010), these phenomena include the role of both technology changes and third-party advocates in making consumer privacy protection a market-reputation issue. The importance of the professionalization of privacy officers as a force for transmitting consumer-expectation notions of privacy from diverse external stakeholders, and related "best practices," between firms is another phenomenon the authors mentioned.

Law has a profound impact on healthcare since it offers a means of assuring that major advances in care are implemented in a manner consistent with equally important economic and social goals (Rosenbaum et al., 2005). However, critiques of the legal framework of privacy in the U.S. and Canada have attacked several aspects of the laws, particularly, their adequacy (often compared with OECD privacy principles). For example, Bamberger and Mulligan (2010) noted what scholars and advocates have charged the U.S. law and wrote:

The dominant critique denounces the existing patchwork of privacy statutes as weak, incomplete, and fractured. It decries the absence of an agency dedicated to data protection and the consequent lack of clear guidance, oversight, and enforcement. And it argues that the U.S. privacy framework fails to provide across-the-board procedures that empower individuals to control the use and dissemination of their personal information.

(p. 249)

Some have even gone as far as stating that U.S. privacy law and its enforcement are fragmented and depart frequently from a "Fair Information Practice Principles" understanding of the meaning of privacy. There are perhaps lessons to be learned from Canada's neighbor about what not to do. While the dominant account argues for greater uniformity and specificity in privacy law, there are others who have suggested the possibilities offered by governing privacy through flexible principles. The authors, Bamberger and Mulligan (2010) also wrote that since 1994, no one had conducted a sustained inquiry into how corporations actually manage privacy and what motivates them. They augmented their position on the lack of interest in privacy matters by adding that privacy decisions were left to midlevel managers who lacked substantive expertise, played particularly subservient roles in most privacy discussions and responded piecemeal to issues as they arose. Failure to spark the privacy engine has been attributed to ambiguity regarding the legal meaning of privacy and the requirements governing its protection in the context of corporate data management. Bamberger and Mulligan (2010) argued that the primary objective of regulatory intervention must be the reduction of ambiguity in the privacy domain.

In 2011, the actress Scarlet Johansson was a victim of phone hacking (Forrester Research 2013).

Her comments about her experience perhaps typifies the legal entitlement most people have about their privacy:

“Who doesn’t want to protect their own privacy? Just because you are an actor or make films or whatever doesn’t mean you are not entitled to your own personal privacy. If that is seized in some way, it feels unjust. It feels wrong”. (Forrester Research, 2013, p. 2)

Effective management of patient information privacy around the world has been promoted and supported by several organizations and legal compliance instruments as well as standards.

Common among these are the *Health Insurance Portability and Accountability Act* (HIPAA) enacted in 1996 in the United States that had a deadline for compliance with the new privacy rules set for April 14, 2003 (Forrester Research, 2013). In Canada, HIPAA is a legislative initiative that mandates the development of national privacy law, security standards, and electronic transactions standard and provides penalties for standards violations and wrongful disclosures of health information (Buckovich et al., 1999). Generally speaking, the Privacy Rule (of HIPAA) protects individual’s personal health information by dictating how and when a person’s personal health information may be disclosed and for what purpose, and grants individuals more involvement by allowing them specific right to access their medical records and request amendments, to authorize or restrict the disclosure of their information under certain circumstances, to be informed of the way in which their information is shared with others, and to be informed of their rights to privacy (Choi et al., 2006). Buckovich et al. (1999) remarked that other contributing factors to the heightened awareness to patient information privacy included

the 1995 European Union's enactment of the *Data Privacy Directive*, which required that all 15 European Union member states establish national privacy laws by October 1998.

In England and Wales, the *Health and Social Care Act* (HSCA) was passed in 2003 leading to the establishment of the Patient Information Advisory Group (PIAG), and the National Health Service Information Authority (NHSIA) that consulted with the public on the privacy of patients (Chalmers & Muir, 2003). The *Personal Information Protection and Electronic Documents Act* (PIPEDA) was implemented in Canada in 2000 to protect patient privacy (Government of Canada, 2020b). Also, the CNA (2008, 2017) is an organization with an interest in patient information privacy. The PIPEDA applies to the personal information collected, used or disclosed by organizations engaged in commercial activities, from banks and retail outlets to airlines, communications companies and law firms. The Act, enacted in 2000, has been fully in force since 2004, applies to private enterprises across Canada (Government of Canada, 2020a). Many private enterprises operating within British Columbia, AB and Quebec are covered not by PIPEDA but by similar provincial statutes. But, even in those provinces, PIPEDA applies to organizations under federal jurisdiction. Other laws and legislature that provide for the protection of privacy in Canada include the *Privacy Act, 1982*, *Personal Health Information Protection Act (PHIPA)*, *Freedom of Information and Protection of Privacy Act (FIPPA), 2000* provincial privacy laws (general), and *Charter of Rights & Freedoms, 1982*. Some of these laws and acts will be discussed in detail subsequently. Among the institutions responsible for protecting the privacy of health information are the privacy commissioner, government ombudsman, hospitals/health care providers, human rights commissioner, provincial bodies (general), professional associations (general), government health departments, institutions related to health,

banks, Canada Revenue Agency, law enforcement, justice agencies, and consumer protection agencies. Although electronic data is rarely 100% secure, the rigorous requirements set forth by legislation make it very difficult for electronic data to be accessed inappropriately. For example, all electronic health records systems must have an audit function that allows system operators to identify each individual who accessed every aspect of a given medical record. Electronic health records continue to be important and many healthcare facilities are converting from paper-based systems.

Although HIPAA started in a paper-based environment, as physicians' offices, medical centers, hospitals, and other healthcare providers began to convert their patient records to an electronic information exchange environment, privacy concerns regarding the sharing of digital records prompted additional U.S. legislative actions. Subtitle D of the HITECH Act includes several provisions strengthening the civil and criminal enforcement of the HIPAA rules.

In the Acts, privacy is defined as previously stated, with a legal context and adapted to meet local needs. For example, in the province of SK, HIPA, 2003 defined privacy as the right to consent and revoke consent to use and disclosure, the right to prevent access to a comprehensive health record, the right to be informed by trustees about anticipated uses and disclosures, and the right to be informed about disclosures without consent (Government of SK, 2020a). However, Canada's Privacy Act only provides investigative authority to the commissioner; this Act has no enforcement tools (Hebert et al., 2010). They reiterated that the Act does little to address the many nuanced privacy issues in dealing with sensitive health information, which explains why several provinces have developed their own privacy laws for health information. The role of ethics in maintaining and supporting the legal ramifications of privacy is worth noting.

Ethics is foundational to nursing and nurses have been noted to uphold ethical values. According to Riffkin (2014), the annual Gallup poll has, on more than one occasion ranked nursing as the most ethical and honest profession. Privacy is a core value deeply rooted in the nursing profession's history and traditions (CNA, 2008, 2017). Respect for patient information privacy as a core tenet in nursing practice is often clearly expressed in the *Code of Ethics* for nurses. Erickson and Millar (2005) believed that nurses' commitment to protecting patients' privacy must advance from the abstract realm of tacit understanding to a more conscious, active, and visible place, a view that is likely shared by many nurses. The exploratory research of their experiences with regard to patient information privacy and security is a step towards engaging RNs in this very important area of their practice.

The table below, adapted from Forrester Research (2013), provides some indication of how the legal environment of information privacy and security in different sectors has evolved for some of the key players (Canada, United States, United Kingdom, and the European Union):

Table 2.1:
Country Comparison of Privacy Acts

Financial Services Year	Country	Acts
1999	United States	Gramm-Leach-Bliley, Title V
2002	United States	Sarbanes-Oxley Act
Healthcare	Country	Acts
1996	United States	Health Insurance Portability & Accountability Act (HIPAA)
1997	Canada	Personal Health Information Act (PHIA)
Privacy	Country	Acts
1974	United States	Privacy Act
1980	OECD	Privacy Guidelines
1995	European Union	Data Protection Directive
1997	OECD	Cryptography Guidelines
1998	United Kingdom	Data Protection Act
2002	OECD	Security Guidelines
2003	Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)
United States Homeland Security	Country	Acts
2001-2004	United States	Homeland Security Presidential Directives (HSPD 1-12)
2001	United States	Patriot Act
2002	United States	Federal Information Security Management Act (FISMA)
2005	United States	Cyber Security Standards plus Reliability Functional Model

(adapted from Forrester Research, 2013),

The introduction of information systems and electronic health records has brought with it some legal awareness and challenges in the healthcare industry. This may be the result of the very nature and capabilities of the technologies. Rosenbaum et al. (2005), identified several distinct characteristics of the health information systems, each of which may raise their own legal questions. There were two common threads among these systems. First, they have the potential to produce large amounts of information about the total health care process experienced

by patients across the domains of health care. Secondly, they have the ability to transfer large amounts of information across the health care system and government agencies. The distinct characteristics as identified by Rosenbaum et al. (2005), which are not mutually exclusive, include decentralized and centralized systems, administrative and clinical data exchange systems (uses of data), and access to the system.

In a decentralized system, the data generated from a query are not stored in a permanent record or central database but in virtual existence and solely for the use of that specific health care provider making the request. Data query works like unrecorded conversation between two individuals. Information is not stored locally. There is however, an audit trail of who made the inquiry. A centralized system standardizes and stores data in a central database. Queries from other providers are essentially captured and stored locally for further use. In administrative and clinical data exchange systems, the intention is to reduce health care administrative costs by enabling providers and insurance organizations to exchange information necessary for payment purposes. Rosenbaum et al. (2005), pointed out that a key distinction in considering legal issues arising from health information has to do with the purpose for which data are used. Other than confirmation of payment and other related services, administrative data exchange system also captures other information such as patient address, etc. This could sometimes pose problems.

Clinical data exchange systems offer patient-specific information at the point of care. These systems share patient information such as demographics, medical records, laboratory, radiology, pharmacy, etc. Such exchange generally occurs on an institution-to-consumer or institution-to-physician basis. Regarding access to the system, the method by which access is provided to the

health information system is a distinguishing characteristic. Access can be regulated through contracts that link health care systems who agree to enter into legally binding agreements.

Contracts often detail who can or cannot use the system and for what purposes, who owns the system, the software used to run the system, and applicable security standards. According to Rosenbaum et al. (2005), specific legal questions may arise depending on the system's structure and uses, and access-related considerations. Questions include whether the system is structured to comply with cross-border provincial or federal government laws, ownership, whether information use procedures conform to applicable laws, what applicable privacy safeguards are in place, and establishment of special procedures for information access under special circumstances.

The longstanding (over one hundred years) link between health information and the law has been particularly visible in the privacy context (Rosenbaum et al., 2005). The use of electronic information technology has exacerbated legal debates as a result of the potential size of damage that could be caused by these systems. Rosenbaum et al. (2005) have grouped the longstanding legal principles into eight major categories related to the overarching themes of privacy and health care accountability. Each category raises distinct legal questions. The categories include: Questions regarding the ownership of health information; questions regarding the appropriate use and disclosure of personal information to third parties; questions regarding the power of government to compel the collection and disclosure of personal health information as part of public health oversight or law enforcement; questions regarding the power of health insurers to compel the collection and disclosure of data as a condition for payment or other purposes; questions regarding data access as a result of privately-mounted civil litigation claims;

questions regarding data access by government law enforcement agencies to support civil or criminal investigations; questions regarding the use and ownership of personal health information for biomedical, behavioral, and health services research as well as the corollary fiduciary duties of disclosure and notice of conflict of interest to the patient when such health information yields important research potential; and questions regarding the legality of race and ethnicity data collection by the government or private industry for quality improvement purposes. The authors have provided clear and concise examples of these categories (Rosenbaum et al., 2005).

The legal environment surrounding health information can be complex due to the multi-level and multi-dimensional legal systems (OPC, 2018). In Canada and the U.S., both provincial and federal, state and federal laws respectively, could be invoked where health information is concerned. Sources of law such as judge-made common law, constitutional principles, jurisdictional statutes, and regulations imposed by the many government organizations can further complicate matters (OPC, 2018). In some cases, the interpretation of federal laws has to be done side by side provincial or state laws. For example, in the U.S., state laws may take precedence over federal laws if the state law provides a more stringent protection (OPC, 2018). Further, electronic health information with the ever-changing information enterprise has brought with it questions never before thought of as being part of the law of health information (OPC, 2018). Even the idea of compliance can be easily misconstrued. For example, if a provider claims compliance with health information laws, what kind of compliance would the entity be referring to? Is it compliant for privacy purposes? Is it compliant with respect to electronic data

interchange purposes? Is it compliant for security purposes? Perhaps, what the law is not able to adequately address, ethics could compensate for (OPC, 2018).

As indicated earlier, core virtues and values of the nursing profession, as well as nurses' duties and responsibilities are represented by international and national codes of ethics in nursing (Rchaidia et al., 2009). Nurses protect the confidentiality of patient information, and respect patients' privacy. Their ethical and professional conduct is guided by nurses' code of conduct in Canada. In some cases however, basic ethical principles such as the sanctity of life, respect for an individual's bodily security, and respect for personal information can be applied. Such principles could be invoked in deciding whether a nurse behaved ethically in a particular situation. Wheat (2009) commenting on the Hippocratic Oath has reiterated that the health care professional has an obligation of beneficence (to do good) and of nonmaleficence (to do no harm). While most would agree with that, he pointed out that the difficulties that arise are in the interpretation of what constitutes "good" and "harm". In extending Wheat's discourse, one could ask the question of how nurses rate the issue of patient information privacy and whether this information has the potential to do good or harm.

When discussing the interplay of ethical principles, Wheat (2009) suggested that perhaps the best way ethics operates in practice is that there is usually more than one particular ethical principle at play. She gave the example that healthcare professionals are aware that the law pertaining to privacy and confidentiality forbids disclosure without consent or a good reason for breaching the obligation of confidence. She further pointed out that the obligation has ethical connotations based upon the respect for autonomy and privacy, and upon the utilitarian principle that people are more likely to seek medical advice if they know that their information will remain

confidential. Thus, judgment calls by nurses relating to patient information privacy would vary depending on what worldview an individual holds or is working with. Such judgment calls could often result in ethical dilemmas in decision making.

Ethical dilemmas in nursing abound, given that each of us has a moral lens by which we view the world. The choices we make in ethical situations is often based on our upbringing, culture, spiritual perspectives, peer group values, and other factors unique to us (Ohio Nurses Association [ONA] 2013. The author continues that, no matter what our personal moral views might be, employers establish policies regarding appropriate behavior in the workplace that ultimately become our “organizational ethics”. Also, as mentioned earlier, professions have standards expected of their members, often referred to as “professional ethics” (ONA, 2013). Are there tensions or conflicts that exist between organizational ethics and professional ethics for practicing nurses in the area of patient information privacy, and are these tensions/conflicts perceptual or real? Is there a clear line of demarcation between the two in the way they operate? Health care employers have “opt out” options for nurses who do not wish to participate in some aspects of patient care (ONA, 2013). This gives the nurse the opportunity to advise his or her manager regarding not wanting to participate as a result of moral conflict.

The ONA (2013) in the United States (not to be confused with Ontario Nurses Association in Canada [ONA]) has provided a brief but interesting discussion on the theoretical frameworks from a historical perspective with respect to clinical ethics decision making. According to the author, virtue ethics is based on what people believe to be required of them in order to be virtuous. Virtue ethics has to do with being excellent in moral reasoning and behavior (ONA, 2013). The author makes it clear that in reality, realizing this ideal could lead to frustration and

stress because people fall short of their perception of perfection. In causistry ethics, what happened in previous cases is used as a guide for deciding what should be done in a current case (ONA, 2013). This approach addresses the reality of a particular situation and looks for consistency in judgment from case to case. The downside of this approach is that not all cases are alike, and differences may outweigh similarities.

Another ethics framework commonly used is utilitarianism, sometimes also referred to as consequentialism (ONA, 2013). Here, the focus is on the value of the consequences of a decision rather than what should be done or has been done in previous cases. According to ONA, utilitarianism seeks reasonable answers to the question, “what is the perceived value of the decision’s consequences to the greatest number of people?” (ONA, 2013, p. 8). Deontological ethics perspectives are based on rules and duties. Rational thought is the focus of this framework. Reason rather than emotion drives this framework. The principalism framework is based on basic principles that guide actions and decision-making. According to the ONA (2013), most people who use this framework have become familiar with four principles that are foundational to ethical issues in the clinical setting. These are autonomy, nonmaleficence, beneficence, and justice.

Following the reasoning espoused by ONA, autonomy is based on the patient’s right to be self-directed. Protection of privacy and confidentiality has been provided as an example of the way this principle is operationalized. Nonmaleficence as mentioned earlier means “do no harm” (ONA, 2013). The intention is to avoid harm or at least minimize it. Important to note is that there are certain situations, sometimes referred to as “double effect”, where it is impossible to avoid harm. The code of ethics for nurses that emphasizes the responsibility of the nurse to

practice with compassion, and respect for dignity, worth, and uniqueness of every individual is a good statement regarding the “do good” principle (ONA, 2013). The principle of justice requires that people are provided with the same options about their care without taking into consideration cost, and discriminatory barriers such as culture (ONA, 2013). This principle does not focus on treating everyone equally, due to the uniqueness of each clinical case. It is noteworthy that autonomy, doing good, avoiding harm, and advancing equity are often in competition with each other. Care is needed in their appropriate management.

2.3.6.1 Feminist Ethics. A relatively newer theoretical perspective in ethics is caring or feminist ethics. This approach uses the traditional female-based problem-solving processes that takes into consideration stakeholder’s perceptions, values, and needs. Emotions play a key role in this approach more than any of the other theories mentioned previously. The ONA (2013) has suggested that due to the complex nature of today’s healthcare environment and ease of access to technology, a blend of approaches should be preferred to only one theoretical framework.

2.3.6.2 Moral Distress. Nurses sometimes suffer moral distress, a phenomenon that occurs when they feel that there is disconnect between what they feel ought to be done and what they are able to do (ONA, 2013). This psychological disequilibrium takes place when the nurse feels she or he has provided care short of the best for a patient whether by omission (appropriate care is not provided for whatever reason) or commission (nurse perceives the care provided as not being right). Moral distress can translate into physical or emotional stress (American Association of Critical Care Nurses [AACCN], 2008). Writing about control in nursing practice, Weston (2010) advocated for autonomy for nurses in decision making situations and commented that autonomy in nursing includes the ability to act according to one’s own knowledge and judgment, taking

into consideration the framework of pertinent laws, rules, organizational policies and procedures.

She also advocated for nurses to participate actively in strategies that will empower nurses to effect change, such as formulation of policies, and process improvement initiatives.

2.3.6.3 Ethical Dilemmas. Nurses do not only have to have knowledge related to ethical dilemma but are also accountable for applying skills learned in this area. According to the ONA (2013), nurses are expected to be familiar with the Code of Ethics for nurses. They also need to have a good understanding of ethical theories and perspectives related to clinical dilemmas. Their understanding of how to get assistance in this area is also important. The Ohio Nurses Association (ONA, 2013) makes reference to the Ohio Nurses Association's 2006 process guide for assisting registered nurses in working through ethical dilemmas.

There are several ethical issues nurses face. Park (2009), cited Christensen's, 2002, review study in which he identified six ethical and legal issues that oncology nurses in hospitals face. Of interest, two of them, documentation and privacy, and informed consent relate to patient information privacy and security. In the literature, mention of ethical dilemmas regarding nurses has often focused on clinical matters such as medication errors with little attention given to privacy and security concerns. Nurses in hospitals reported that they experienced frequent ethical problems related to patient confidentiality or privacy issues (Park, 2009) but the author did not elaborate on the details of what aspect of this area their experiences were. Park's review also found that perioperative nurses experienced more frequent ethical issues related to protecting patient rights and human dignity, and informed consent than other issues.

Regarding the approaches and resources that nurses have for solving ethical issues, Park's (2009) found that most nurses used their own personal values to solve ethical issues. Most nurses also

discussed ethical problems with nursing peers. A limited number of nurses were reported to have talked to a higher administrative authority concerning an ethical issue. According to Park (2009), a number of articles reported on the nurses' educational need related to nursing ethics. Some of the need areas reported were professional responsibility, patient rights, ethical code/principles, patient advocacy, and ethical decision making.

Among the skills necessary for clinical dilemmas recommended by the American Society for Bioethics and Humanities (ASBH, 2011) are assessment and analysis of ethical issues, process skills for guiding conversations and problem solving, facilitating formal meetings, evaluation and quality improvement, and interpersonal communication. Knowledge areas recommended were: moral reasoning and ethical theory; common bioethical issues; healthcare systems in general; clinical context for particular cases; facility policies, processes relative to a particular case; beliefs and values of the population being served by the facility; relevant codes of ethics or professional conduct and accreditation standards; and relevant health laws (ASBH, 2011).

In nursing, it is believed that being able to apply the professional principles of training influences work satisfaction (Biton & Tabak, 2003). These principles often emanate from the nursing ethical code of conduct. However, the everyday strain of a nurse's work is likely to compromise the amount of energy dedicated to following the ethical code. Biton and Tabak wrote that work satisfaction relates to one's emotional evaluation of experiences during work. They remarked that the gap between the ethical requirements as perceived by the nurse, and the perceived extent to which they are applied will influence work satisfaction through the mediating

effect of role conflict. The authors added that demographic factors such as age, tenure, and number of children could also exert an effect.

Biton and Tabak (2003) claimed in their study that examined the perceived gap between the ethical code's decrees and the nurse's perceived ability to actually implement the ethical code at work of Israeli nurses that, one of the biggest challenges facing the nurse as a professional is the correct and moral implementation of the nursing ethical code of conduct. They emphasized that the nurse is constantly confronted with dilemmas which are not included within the framework of the ethical code. Their study focused on the value of privacy and provided examples of daily dilemmas nurses face such as delivering of information regarding patients through the phone and providing information regarding the patient within hearing range of other patients. Biton and Tabak (2003) expressed the importance of privacy to a nurse and the inadequate attention in this area by stating that "privacy is an important part of a nurse's ethical code, but because it is not a life-or-death issue, it does not usually take priority in patient care".

This may translate to lack of support for nurses when it comes to implementing privacy initiatives and consequently lead to their frustration. Biton and Tabak (2003) citing Wilson, 1987, have written that an inability to implement ethical rules at work was one of the main reasons nurses abandoned the profession.

A nurse's own skills and knowledge are not necessarily the factors that affect his or her ability to act in accordance with the ethical code. There are several external factors not related to the nurse's personality that, according to Biton and Tabak (2003), influence action. These environmental factors include multiple expectations. The nurse has to satisfy the patient, the organization, and medical personnel. Complexity of the ethical code is another factor. The code

may spell out extensive obligations not only to fellow nurses but to the hospital, superiors, patient's family, oneself, and to society. Another factor worth considering is organizational constraints. The prevailing management or organizational culture in a medical or nursing unit may hinder appropriate implementation of ethical rules.

2.4 Social Media, Nurses, and Information Privacy

Social media has been described as a collection of online communications channels dedicated to community-based input interaction, content-sharing, and collaboration (Wise & Shorter, 2014). Social media are essentially websites and applications committed to forums, microblogging, social networking, social bookmarking, social curation, and wikis, to name a few. Another definition of social media that appears to be a refinement of that provided by Wise and Shorter and brings out its participatory nature is “a group of internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content” (Kaplan & Haenlein, 2010, p. 61). Examples of social media include Facebook, Twitter, Google+, Wikipedia, LinkedIn, Whatsup, and Reddit. Whatis.com (2015) has provided brief descriptions and examples of the different social media types. Kaplan and Haenlein (2010) have characterized the many forms of social media into six main types and provided examples for each main type. Leadgenera.com (2020), has provided and briefly described what the organization considers the top social media and Content Applications for 2020. These applications include: Facebook, Instagram, Twitter, Youtube, ContentCal, Hootsuite, Canva, Captiona, Story Slicer, and Planoly. There are many more social media platforms available to the public, including nurses.

Social media affords their users, including nurses, several undeniable benefits. Such benefits include networking and building nurturing relationships among professionals, exchange of knowledge and new ideas related to nursing and health care in the area of education, research and best practices, and also public education on nursing and health related matters. The power and pervasiveness of social media is significant. Barry and Hardiker (2012) using figures provided by NielsonWire (2010), estimated that globally, over 20% of internet time was spent on social network and blogging sites and twitter generated over 340 million tweets daily. The World Health Organization (WHO) is using its facebook, twitter, and You-Tube presence to counter rumours and to inform the global public of outbreaks (Barry & Hardiker, 2012). According to these authors, the United Kingdom Nursing and Midwifery Council estimated that there were about 355,000 registered nurses and midwives on facebook alone in the UK.

Regarding the use of social media by nurses, Kerr et al. (2020) have documented how some nurses have attained what they termed “microcelebrity status” in the nursing community using social media such as Instagram. According to the authors, this level of popularity has elevated the nurses to “Influencers” and “Opinion Leaders” often with significant following (Kerr et al., 2020). In another study that explored the ways occupational health nurses can use social media as a helpful resource as well as identify potential concerns associated with its use, Siegmond (2020) found that social media can be used for encouraging participatory health care among employees, health information, online health communities, emergency communication, health education workshops, professional connections, and continuing education. The possibility of misinformation and privacy breaches were some of the downside of the use of social media.

Social media however, constitutes a source of many challenges for a professional. With the growing use of internet social networking sites among nurses, the frequent access nurses have to mobile phones, computers and tablets, the need for appropriate use of social media should continue to be important. In some parts of the world, the increasing complaints to boards of nursing regarding the misuse of social media by nurses, often to the extent of violating patient information privacy and confidentiality has elevated this need to another level. As has been mentioned repeatedly throughout this review, nurses have many personal rights and freedoms. They are also privileged members of a regulated profession with a responsibility to uphold patient trust, confidence, and privacy (Iowa Board of Nursing [IBN], 2014).

Social media offers an easy platform for a nurse's personal actions to collide with professional responsibility. Incidents of nurses taking pictures with their cell phones and posting those pictures on Facebook, and getting involved in other ethical breaches are many. According to IBN (2014), a survey by the U.S. National Council of State Boards of Nursing (NCSBN) in 2010 found that, of the 46 boards surveyed, 33 reported complaints regarding breaches.

In order to minimize or eradicate such incidents as mentioned above, many nursing boards and associations have come up with guidelines and tips regarding the use of social media (British Columbia College of Nursing Professionals, 2018; CNPS, 2010; IBN, 2014; NCSBN, 2014; Nursing and Midwifery Board of Australia, 2010; Nursing and Midwifery Council, 2011). Barry and Hardiker (2013) have also listed a number of relevant publications that address issues regarding the use of social media by health care professionals. Cases of inappropriate use of social media may often be reported to Boards of Nursing. Disciplinary action depends on the laws pertaining to a jurisdiction. Generally, investigation of cases of inappropriate behavior may

be conducted on the grounds of unprofessional conduct, unethical conduct, moral turpitude, mismanagement of patient records, revealing a privileged communication, and breach of confidentiality (NCSBN, 2014). Disciplinary actions include reprimand or sanction, assessment of monetary fine, or temporary or permanent loss of licensure. In some cases, civil or criminal penalties may result when a nurse breaches patient confidentiality or privacy. Misuse of social media can also affect the reputation of the organization.

The NCSBN (2014) has commented that most social media misuse that has occurred was inadvertent and has attributed such instances to a number of factors. According to NCSBN, there is a mistaken belief that the communication or post is private and accessible only to the intended recipient. There is also the illusion that deleted content is no longer accessible. Some even believe that content received by the intended recipient is harmless as long as it is between the two individuals communicating. Others have the mistaken belief that it is acceptable to make reference to patients as long as they are not identified by name but use other attributes such as diagnosis or condition. The ease of posting and sharing information using social media was mentioned as another factor. The NCSBN (2014) has made several suggestions with practical scenarios to help avoid the problems indicated above.

According to Forrester Research (2013), generation Z, those that are 18 to 23 years old, has no concerns about sharing some of the most intimate facts about themselves on Facebook.

For example, 4.7 million individuals have “liked” a Facebook page about specific health conditions or treatments, 4.8 million used Facebook to say where they planned to go on a certain day, 20.4 million included their birth date, 900,000 discussed finances on their Facebook.

2.5 Information Privacy Breaches

As indicated earlier, a breach is the breaking of a rule or law or the upsetting of a normal and desired state. Information privacy breach could therefore be defined as any act that is contrary to established information privacy laws, rules, regulations, standards, and similar mandates designed to protect information privacy. After a number of high-profile privacy breaches and missteps such as the news of the world phone hacking scandal and Google's bypassing the browser privacy settings of Apple Safari users, governments, industry regulators, and the public have become increasingly aware and sensitive to privacy issues. The US Federal Trade Commission fined Google \$22.5 million, the largest fine it has ever levied (Federal Trade Commission, 2012). The motivation for intentional privacy breach is not difficult to understand. In the underground market economy, data is money, and much like any other market economy, principles of supply and demand drive it. Simple identity theft pays about \$2,000, on average, but a thief using a medical ID number can earn an average payout of \$20,000 for a medical record (Forrester Research, 2013). In 2010, the Privacy Rights Clearinghouse's Chronology of Data Breaches (PRCCDB, 2015) reported more than one half billion sensitive records breached since 2005. Such breaches involved, among other things, medical records. The publisher added that the number was conservative as it included only those breaches that received media attention.

A search using the interactive online of the PRCCDB (2015) revealed that in the past five years, 26,797,057 medical records breaches have been recorded in their database, from 975 data breaches made public. This number is for the different regions in the U.S. alone. These breaches include unintended disclosures, hacking or malware electronically from outside, insider with

legitimate access intentionally breaching information, physical loss as a result of lost or stolen non-electronic records, loss of portable devices such as laptops, lost or discarded stationary devices, and unknown sources of breach. Of the total mentioned above, 1,335,739 breached records of 300 breaches made public resulted from unintentional disclosure and insiders with legitimate access (PRCCDB, 2015). Medical record breaches could occur anywhere and is an ongoing concern, as the reported incidents below would suggest.

Radio New Zealand (2015) reported discovery of 20 years old confidential medical records in an unoccupied house that were subsequently handed over to a district health board. In Canada, there are calls to take privacy laws seriously and to prosecute those snooping into patient's medical records. In an editorial, Toronto Star (2015a) remarked that the Personal Health Information Protection Act has been in force for more than 10 years and no one has ever been successfully prosecuted in Ontario for violating its terms. The writer claimed that several troubling breaches have been made public in recent months. The editorial gave an example of two employees at Rouge Valley Centenary Hospital who were caught supplementing their income by passing information on thousands of new mothers to businesses hoping to sell them their services. In another instance, the editorial mentioned that five staff members peered, without good reason, into the records of 22 patients at the Centre for Addiction and Mental Health (Toronto Star, 2015a). The Toronto Star (2015b) also claimed that former Mayor Rob Ford's medical records had been inappropriately accessed no less than four times since his cancer diagnoses, and yet, none of these matters had resulted in any charge for breaching the health information act. The editorial concluded that the justice system lacks the willingness to pursue such violations. Perhaps Ontario is not alone in matters of this nature. The Times Colonist

(2015) insinuated similar sentiments regarding the willingness of the government to act decisively when it came to breach of privacy laws. The Times Colonist reported what seemed to be a reluctance of the government of British Columbia to forward a health ministry privacy breach investigation to the Royal Canadian Mounted Police (RCMP) in 2012.

In some cases, the perpetrators of breaches linger to collect as much information as possible. Such was the breach that occurred at Healthfirst, a health care provider in the U.S. where data for 5,300 patients were stolen from their online portal between 2012 and 2014 (Office of Inadequate Security, 2015). Information believed to have been accessed included patient name, address, date of birth, health insurance plan information, physician number, member ID, patient ID, claim number, and diagnosis code. In another “lingering” breach incident, Global News (2015) reported that the Prince Albert Parkland Health Region (PAPHR) in Saskatchewan, Canada, said an employee not providing care to those patients accessed medical records of 16 patients between January and December of 2014. The Lakeridge Health Services in Ontario, Canada, notified 578 people in November of 2014 that their health records had been inappropriately accessed (Northumberland News, 2014). According to the news agency, 14 staff members who provided mental health services accessed this information for a 10-year period between 2004 and 2014. The president and CEO of the facility suggested that perhaps it was an innocent check by previous staff and that staff rationalized it as “it’s just my eyes”. The Calgary Herald (2014) reported a breach incident in which a staff member at the Alberta Children’s Hospital inappropriately accessed nearly 250 patient files over a 14-year period.

Metro News (2015) reported that a health authority in Newfoundland and Labrador was investigating a breach in confidentiality after a document containing patient information was

picked up from hospital property in Grand Falls, Windsor. Hundreds of medical records have also been found scattered around a busy street for about a week in Richmond Hill, Canada (City News, 2015). The Peterborough Examiner (2015) reported a privacy lawsuit against Peterborough Regional Health Centre, in Canada. According to the report, the estimated general, punitive, and aggravated damages was \$5.6 million. The lawsuit was as a result of inappropriate access to medical records of 280 patients. There is even black market for stolen health care data with well-established websites. The National Public Radio (NPR, 2015) reported that one particular website had a value pack that included 10 people's medicare numbers for \$4,700.00.

The quest to find out about the private lives of public figures is another reason health record information breaches occur. Health professionals have been caught snooping into former Mayor Rob Ford's medical records in four separate privacy breaches in at least three Toronto hospitals since his cancer diagnosis in September of 2014 (Toronto Star, 2015b). In the same report, the Toronto Star (2015b) mentioned that their recent investigation found that majority of health-related breaches go unreported to the privacy office. Nearly all 218 privacy breaches uncovered, which occurred at just eight of Toronto's biggest health institutions were not reported because of what has been called a legislative loophole (Toronto Star 2015b). Under current law, hospitals can handle privacy violations without informing a regulatory body (Toronto Star, 2015b). The report commented that eight jurisdictions had recently amended their health privacy laws to fix this problem.

A day after news that Toronto Mayor Rob Ford's records were inappropriately accessed, former NDP leader, Jack Layton's wife confirmed that her husband suffered a similar fate while he was in the care of another major Toronto hospital (Globe and Mail, 2014).

Breaches have also been motivated by social activist agenda, as was the case when an anti-abortion activist inappropriately accessed more than 400 abortion files at the Peterborough Regional Hospital in Ontario, Canada (Toronto Star, 2015a). In this article, the Toronto Star claimed that there were 155 hospitals in Ontario, and every year, the privacy commissioner's office receives about 400 notifications of health-related privacy breaches. Such cases of privacy breach where the primary aim is curiosity, abound.

The Vancouver Sun (2014) reported on an investigation in which two employees viewed the confidential electronic health records of 112 people to satisfy their personal curiosity. The report suggested that there are perhaps thousands of unreported violations. If this is the general trend in the other provinces, one could conveniently say that there is work to be done.

Other breaches appear to be the result of carelessness. The case of an Edmonton man who was discharged from the Royal Alexandra Hospital, Edmonton in Canada with another patient's discharge papers, was simply carelessness or the lack of attention (Global News, 2014).

In most breaches that occur, the identities of the offenders, whether a category of staff or individuals, are often not divulged. However, there have been incidences of breaches where nurses have been explicitly mentioned. The Gaston Gazette (2015) in the U.S. reported a breach in which a nurse (a pastor's wife) pleaded guilty to identity theft. According to the report, the nurse offered to help the victims who were members of their congregation. The nurse reportedly accessed the victims' medical and personal records and used this information to make purchases with the victims' credit cards, among other crimes.

Another blatant case of medical identity theft by a nurse occurred in the U.S. where the nurse stole personal information of 20 patients and used that to file fraudulent claims

(Washington Association for Bilingual Education [WABE], 2015). In the U.K., a nurse with 30 years' experience was suspended from working as a nurse and dismissed for breach of confidentiality that involved accessing medical records of a patient she had no clinical involvement with on four different occasions, and discussing them on social media (Chronicle Live, 2015).

In Lakewood Ranch, U.S., a registered nurse working in the emergency room was fired and arrested for using a patient's credit card information to make personal purchases (Herald Tribune, 2014). A police search at her home lead to the discovery of a handwritten ledger listing personal information and credit card information for about 20 former patients.

A nurse in New Zealand was fined \$6000 for inappropriately accessing electronic clinical records of patients on 19 occasions without authority over a period of 8 months. She admitted to the charge and said she knew it was wrong (The Press, 2014). She however attributed her actions to significant workplace stress that caused her to lose professional judgment. The report related that the nurse involved was a highly experienced charge nurse, with over 40 years of nursing experience. Of interest, it was also mentioned that the nurse reported her own misconduct to her employer.

When it comes to patient information privacy, health professionals and administrators appear to have dissenting attitudes towards preventing, detecting, and dealing with breach. While some have gone to the extent of making public declaration to show their commitment to ensure privacy, there are others who appear to be slow in responding to privacy initiatives. For example, the attitude of the Minister of Health and Long Term Care for Ontario, Canada, when he said "Even one privacy breach is too many, and we will continue to work across the health sector to

ensure that the personal health information of Ontarians is protected” (Toronto Star, 2015a, p. 6), speaks for itself.

The Toronto Star (2014) conducted an investigation after a number of high-profile breaches involving Toronto hospitals and found that several hospitals did not proactively audit staff access to confidential medical records. Providence Healthcare was named as one of the hospitals that still used paper-based record keeping, and the report said that Providence Healthcare could not conduct audits until a future electronic system was implemented. The same article revealed that the Rouge Valley Centenary Hospital suffered a massive breach that affected over 14,000 patients and still lacked the ability to track staff access to confidential files (Toronto Star, 2014).

The Personal Health Information Protection Act (PHIPA) does not specifically require audits. The PHIPA leaves the health care providers to determine how best to comply with privacy requirements, and what disciplinary actions should be taken if a breach occurred. The question of whether people have the right of notification when a breach has occurred has not been fully addressed in Canada, according to Roseman (2014). Roseman (2014) reported that the Heart and Stroke Foundation of Canada faced a dilemma of whether to notify 123,000 people whose names and email addresses were posted on the internet by mistake. She mentioned that breach notification is not required under Canada’s federal private-sector privacy law, PIPEDA.

There have however been occasions when the provincial privacy commissioner has required that health care organizations post notices on their websites advising the affected individuals that their personal information have been compromised (North York Mirror, 2014). For example, Humber River Hospital and North York General Hospital both in Ontario, Canada,

were required by the provincial privacy commissioner to post notices on their websites advising maternity patients that their personal information may have been provided to baby photographers.

2.6 Electronic Health Records

The terms electronic medical records (EMR) and electronic health records (EHR) are often used interchangeably but the literature suggest that they have different meanings (Garets & Davis, 2006). According to Parks et al. (2011), management information systems and medical informatics literature refer to EMR as electronic patient records that are created and maintained by one care delivery organization (CDO) and includes patient medical history, clinical documentation, medications, laboratory, and radiology test results. EMRs may include reminders and alerts, clinical decision support systems, and links to medical body of knowledge and other aids. EMRs are provider-oriented health information systems and are sometimes referred to as physician office systems or practice management systems (Ludwick & Doucette, 2009).

The EHRs capture patient information in digital format and make the information available to other healthcare stakeholders (Angst & Agarwal, 2009). The EHRs allow for interoperability of health information. The EHRs represent the ability to easily share medical information among stakeholders and to have a patient's information follow him or her through the various modalities of care engaged by that individual (Angst & Agarwal, 2009). An EHR may draw on health information sources such as EMRs, drug repositories, centralized lab sources, and other point-of -service applications over many encounters to assemble a complete

health record about a patient (Ludwick & Doucette, 2009). The EMR is a broad range of information from family physicians, specialists, social workers, pharmacists, radiologists, dieticians, physiotherapists, and nurses (Ludwick & Doucette, 2009). Another terminology that is often confused with electronic health records is personal health record (PHR). A PHR is a means of storing, managing, and sharing your personal medical information (Privacy Rights Clearinghouse [PRC], 2012). Individuals have the ability to manage their own PHRs. Privacy Rights Clearinghouse explained that this is one factor that distinguishes a PHR from an EHR. An EHR is one of many individual records contained in an electronic records system that your health care provider controls and populates with information (PRC, 2012). With a PHR you have control over what information you put into it and share with others. According to PRC, this does not mean that you have exclusive control over who can see your medical records or how they are used. Those records all exist elsewhere, in either paper or electronic form, under the control of your health care providers (PRC, 2017).

Different types of PHRs are available; they can be paper-based or electronic (PRC, 2017). In electronic form, the records could be on different media such as computer hard drives, smart cards, thumb drives, CDs, and web-based applications. Paper records may be easier to physically secure but electronic records are more convenient and portable. They are easier to update and maintain and also easier to access and share. The PHR applications can be installed on a computer to record medications and remind the patient when to take them (PRC, 2017). Most PHR products are internet based, for example, Microsoft's HealthVault (Sunyaev et al., 2010).

There are also smart phone mobile applications that have a variety of features for maintaining and managing medical information such as medical history and conditions, diagnostic test results, food and medication allergies, travel history and immunizations, and medication names, doses, frequency, and start/end dates (Ventola, 2014). Some smart phones are even capable of measuring vital signs like heart rate and blood pressure. In some cases, the application may allow sharing information on social media. One would find it easy to understand why these applications that offer convenience could also present numerous privacy and security concerns. There are vendors that supply PHR smart cards for storing medical information.

Electronic medical record usage has continued to advance to the point that now there are associations like the American Health Information Management Association that has a website that can help you choose a PHR based on your age and other health requirements. The National Institute of Standards in Technology (NIST, 2015) has recently published a draft of its first cybersecurity practice guide titled “Securing Electronic Health Records on Mobile Devices” to ensure that doctors and other medical staff do not inadvertently compromise patient data when they use smart phones to access electronic health records.

In order to encourage adoption of electronic health records in the United States, recently updated law requires health care providers with EHR systems to give individuals an electronic copy of their record on request and charge only for the labor cost of responding (PRC, 2012). Empirical evidence has shown that the benefits of computerization were greater than the risks of confidentiality loss (Perera et al., 2011). In addition to improved legibility, the organized note structure of many EMRs supports high quality patient summaries desirable for shared clinical care. In addition, the detailed healthcare information in EMRs makes them important sources of

information for clinical, research and policy questions. Ardito (2014) has provided a brief but useful discussions on the advantages and disadvantages of electronic health records. Edwards (2013) has documented an extensive list of benefits and drawbacks electronic health records bring to healthcare in general. Edwards argues that nurses must continue to trust their instincts and obtain review, even in the event that the system advises that the patient is safe and well. Robey (2014) has identified definite problems in healthcare that EHR can help solve. These included cost, healthy living, personalized care, empowering patients and doctors, crowdsourcing care, population health, epidemiology, drug development, and innovation. The benefits that accrue to the use of EHR systems appears to make their use almost inevitable. Governments have rallied their support for such systems by providing financial and other resources to augment adoption of EHR.

Canada Health Infoway (CHI, 2021), an independent, federally-funded, not-for-profit organization, has been mandated to accelerate the development of EHRs in Canada. The goal of CHI is to contribute to the development of a network of EHR systems in order to enable efficient communication between health care professionals. In addition to creating and certifying software product standards in the health industry, CHI answers questions regarding safety, security, privacy, and ethical implications of EHRs systems. The initiative to move Canadian medical records from a paper to a computerized electronic format has been slow, with mixed results (Davidson, 2009). The CHI noted that eight years after spending about \$1.6 billion in 2001, only 17% of Canadians were using EMR. This was well below the organization's goal of 50% by 2010. Within the same period in the U.S., EHR adoption rate had jumped from 18% to 48% for

office-based physicians (Hsiao & Hing, 2014). As noted earlier, electronic health records system has several implications for patient information privacy.

2.6.1 Electronic Health Records and Patient Information Privacy

Electronic health record use depends on technology, and with information technology, the ability to rely on these same physical, psychological and social mechanisms for regulating privacy is changed and often reduced (Palen & Dourish, 2003). They explained that in virtual settings created by information technologies, audiences are no longer circumscribed by physical space; they can be large, unknown and distant. The authors added that the ability to record and subsequent persistence of information especially that which was once ephemeral, means that audiences can exist not only in the present, but in the future as well. Also, information technology can create intersections of multiple physical and virtual spaces, each with potentially differing behavioral requirements. The background provided above can be revealing. The complex environment created by technology could make the optimal control of information privacy of electronic health records difficult to achieve.

The characteristics of EMR databases that give them their strength, including organization of complex information into standard database format, rapidly accessible key fields, and compact storage of multiple patient's data are often the sources of health information privacy concerns (Perera et al., 2011). The threats posed by information technology, which is the platform for electronic health records, has been recognized by governments. In the U. S. for example, Congress and the Department of Health and Human Services refined the original mandate of "The Privacy Rule" which identifies specific protections that health plans, health care clearinghouses, and health providers were required to implement in accordance with perceived

threats (Informa Healthcare, 2009). According to Informa Healthcare, many experts and clinicians have concerns about how client's privacy rights will be affected by the widespread implementation of Electronic Health Records (EHR).

In a study conducted by Ludwick and Doucette (2009) to understand factors that affect the implementation of health information systems in general practice, several observations were made that could impact patient information privacy and security. Among the concerns that influence implementation success that implementers had was privacy, but the authors did not elaborate on that. In their discussion of socio-technical perspectives of health information systems, they pointed out evidence that there is a relationship between the tools that facilitate the healthcare processes and the interpersonal interactions needed to carry out the day-to-day clinical tasks of a care facility (Reddy et al., 2003). The complex interactions among the players in this environment could result in lapses that lead to information breaches. In the light of breaches in data security in banking, retail, social security, and national security, supported by a similar technological platform as that of health information systems, violations of patients' privacy are easy to envision with the wide accessibility to patient records. Information privacy has been cited as one of the main, if not the main barrier to information technology integration in some areas of the health sector such as psychiatric settings (American Psychiatric Association [APA], 2008). Information privacy concerns are even higher in these areas due to the sensitive nature of client data that is recorded, and the multiple layers of providers with access. Insurance and employment discrimination, stigma, and financial repercussions can result when data are shared inappropriately. The APA (2008) further commented that an understanding of privacy concerns

and standards enables psychiatric mental health nurses to advocate for information systems and policies that protect client privacy yet facilitate the benefits of EHR.

The APA (2008) found that new implementations of electronic health record systems often challenge organizations to build a collective understanding of their processes so they understand how a new system fits. They added that such efforts uncover process inefficiencies. My qualitative study using semi-structured interviewing of registered nurses to explore their experiences in patient information privacy could lead to the discovery of themes that contribute to the overhaul of any such inefficiencies in patient information processes involving nurses. Most often, the staff, not the executives has the best knowledge of existing and optimized processes.

There are other challenges in EHR systems that could be unsettling in relation to privacy. Different countries may have resolved such challenges to different extents. Informa Healthcare (2009) has provided a brief discussion of such challenges in four areas in electronic information exchange faced by the U.S. Among these challenges were: understanding and resolving legal and policy issues, appropriate disclosure, ensuring individual's rights to access and amend health information and, implementation of adequate security measures. Regarding the question of what steps are being taken to protect the privacy of citizens' personal health information, Informa Healthcare (2009), claimed that the European Union, the United Kingdom, Canada, and New Zealand are among the governmental entities that have acted to establish privacy rules. Informa Healthcare (2009) added that in the U.S., a multi-pronged effort was underway expanding well beyond HIPAA (Centers for Medicare and Medicaid Services, 2008; Department of Health and Human Services, 2008). In connection with the role of nurses in patient information privacy and information systems, Informa Healthcare (2009) made a statement worth-noting:

In order to protect patient documentation and security and limit their liability, psychiatric-mental health nurses are advised to review current and potential information systems for compliance and to work with agency and vendor system developers. Nurses' deep knowledge of care processes and outcomes will enable them to make significant contributions by participating in the development of security models, setting standards and guidelines, designing architecture, implementing and evaluating policies, and establishing access restrictions and consumer controls. (p. 409)

CARNA (2020b) has clearly indicated that regulated members are accountable for understanding which legislation applies to their nursing practice. Using a semi-structured interview, it will be interesting to learn what nurses have to say, as well as how they feel regarding aspects of the above statement, knowing that nurses are subject to increasing scrutiny regarding their record-keeping (Edwards, 2013). According to Edwards, plans are in place to revalidate nurses in the U.S every three years, and fitness-to-practice assessments are likely to encompass the quality of documentation. The Nursing and Midwifery Council (NMC, 2011) Code of Practice advises nurses to account for both their acts and their omissions.

In emphasizing the significance of the role of nurses, Edwards (2013) commented that nurses are the 'glue' of health-care practice, spanning the entire care process from admission to discharge and into community settings. They are privy to exchanges with the entire multidisciplinary team and are responsible for coordinating care. Thus, nurses need to be fully conversant with any system of communication to ensure that they can support clinical activities, demonstrate patient care and facilitate review. In addition, patients need to have confidence that their private information will be safe and free from exploitation.

Some have asserted that both Canadian and American governments are moving towards a model where all data will be centralized/archived in large data warehouses (Davidson, 2009). Patient information could also have significant presence in the cloud, by way of cloud computing. Organizations will then be effectively contributing to growing digital medical files of patients and residents. Who will actually own the aggregated data when each caregiver contributes to a growing body of information in a centralized database? Unfortunately, available literature has not addressed this question adequately. Answers to this question would determine the nature, sufficiency, and appropriateness of privacy protection. Davidson (2009) pointed out that conceptually, it could be argued that the data will be owned by the patient or resident since he/she will have to give written approval to grant access. The patient should be allowed to view the contents of the file and have the opportunity to correct any errors or omissions, characteristics crucial to the definition of information privacy. However, patients do not have access to the centralized servers housing their records and thus do not have the opportunity to tidy up errors, omissions, etc. In this sense, privacy, in the true sense of the word is often not exercised.

2.7 Nursing Roles and Patient Information Privacy

Nurses provide the largest portion of direct patient care. Their roles in shaping the design, plan, implementation, and maintenance of patient information privacy cannot be minimized. In order to appreciate the role nurses play in patient information privacy and security endeavors, it is necessary to understand what nurses do in general and in particular, how what they do affects the handling of patient information. This section summarizes pertinent nursing practices and how

they influence or are influenced by patient information privacy and security practices. This knowledge should provide the context in which patient information privacy and security compliance mandates are enforced.

Nursing roles have been variously described in the literature. One way of describing their roles which I found elaborate was captured in a research document. Langland et al. (2010) identified four ways of understanding the nurse's role in interactions with the patient: Focusing on medical treatment, following prescribed instructions, and maintaining routines; providing information, giving service, and coordinating care and treatment; seeing patients as vulnerable people, helping and supporting them as individuals; and, inviting patients to participate in the caring process and encouraging them to take responsibility in their own care. In order to achieve a patient-centered care, the authors encourage nurses to pay attention to all aspects of the interaction. They noticed a gap between what is described in regulations and what is done in clinical practice.

A major part of a nurse's day-to-day activities is handover. Among other things, handover is a communication process that provides direction for nurses beginning their duties and helps maintain consistent and continuity of care. According to Fenton (2006), 'handover' (or shift-change reporting) is an important ritual, a transitional period that symbolizes the transference of responsibility. This transfer includes that of patient information. There are several models of handover. Fenton (2006) outlines the common and relatively easy to follow models proposed by McKenna (1997). The bedside handover report is where patient information is shared at the bedside with the team of nurses coming on duty. The written handover report involves a review of documented information which minimizes the opportunity for face-to-face

discussion. There is also the tape-recorded handover in which those on the new shift listen to a pre-recorded tape. Lastly, there is the office-based handover where information is discussed away from the patient. Which of the handover models should be favored is not the subject of this review and will not be discussed in further detail. The possible implications of these processes for patient information privacy may be worth noting.

The pattern, duration, and frequency of nursing activities may hold important cues to certain behaviors observed among nurses that do not foster or even enhance information privacy practices. Some understanding of this area of nursing could also help use appropriate perspective in interpreting what the nurses are saying during and after data collection for my proposed research. In a study to quantitatively measure the workflow and computer use by medical-surgical nurses, the researchers found that assessing, charting, and communicating were the most frequent activities consuming 18.1%, 9.9%, and 11.8% of nurse time respectively (Cornell et al., 2010). They observed that 40% of the activities took less than 10 seconds. Their observations led them to conclude that nurses constantly switch activities and locations in a seemingly random pattern. Cornell et al. (2010) added that the chaotic pace implies that nurses rarely complete an activity before switching to another. They pointed out that the opportunity to use critical thinking and engage in planning care is severely limited under such circumstances. The frequent switching often caused by unanticipated and urgent demands creates stress and impacts performance.

The workflow of nurses is key to understanding efficiency and improving resource planning and is useful in productivity and technology initiatives (Cornell et al., 2010). Knowledge of nurse workflow provides a foundation for understanding how the role of the nurse

needs to evolve. Of interest to my study is to ascertain qualitatively (perceptions) through my study, the subtle or obvious effects that technology (EHR), policies, or regulations may have on nurse workflow. Such knowledge could lead to better understanding of how the nurse's role impacts information privacy and security compliance.

The environment in which a nurse works is likely to impact work performance including adherence to regulatory compliance. High patient-nurse ratio is often associated with poor work environment. Nurses who worked in poor environments cared for an average of 5.3 patients, while nurses in the better environments had an average workload of 4.6 patients (Kutney-Lee et al., 2009). Poor nurse work environments and staffing levels have been linked previously to nurse turnover. Additionally, Kutney-Lee et al. (2009) claimed that better hospital nurse work environments have been linked empirically with higher job satisfaction and lower nurse burnout.

Nurses assume the major role in determining and implementing acceptable standards of clinical nursing practice, management, research and education (Rchaidia et al., 2009). While in the not so distant past the most important quality of an expert nurse was considered to be the delivery of expert care, more recently, it appears that the emphasis is shifting from the delivery of care to the plethora of roles the expert is expected to fulfil in addition (Roberts et al., 2011). These roles include leader, researcher, teacher, change agent, policy writer, and professional spokesperson. Benner (1984) suggested that there is a wealth of untapped expert knowledge embedded in the practices and knowhow of expert nurses that remains unrealized unless it can be articulated by nurses. An exploratory study will provide nurses the avenue to articulate patient information privacy insights that decision makers can learn from.

Nurses have played several leadership roles and impacted the world in many ways. A notable example is Florence Nightingale, the founder of modern nursing (World Health Organization [WHO] 2020), and a transformational leader. The Canadian Association of Schools of Nursing (CASN, 2012) has outlined their IT expectations for RNs in their publication CASN Entry-To-Practice Nursing Informatics Competencies for Registered Nurses. Some of the CASN (2012) applicable indicators within their three competencies are:

Competency: Information and Knowledge Management

Uses relevant information and knowledge to support the delivery of evidence informed patient care

- Describes the processes of data gathering, recording and retrieval, in hybrid or homogenous health records (electronic or paper), and identifies informational risks, gaps, and inconsistencies across the healthcare system (CASN, 2014, p. 7).

Competency: Professional and Regulatory Accountability

Uses ICTs in accordance with professional and regulatory standards and workplace policies

- Complies with legal and regulatory requirements, ethical standards, and organizational policies and procedures (e.g. protection of health information, privacy, and security) (CASN, 2012, p. 9).
 - Recognizes the importance of nurses' involvement in the design, selection, implementation, and evaluation of applications and systems in health care (CASN, 2012, p. 9).

Competency: Information and Communication Technologies

Uses information and communication technologies in the delivery of patient/client care

- Describes the various components of health information systems (e.g., results reporting, computerized provider order entry, clinical documentation, electronic Medication Administration Records, etc.). (CASN, 2012, p. 11).
- Describes the various types of electronic records used across the continuum of care (e.g., EHR, EMR, PHR, etc.) and their clinical and administrative uses (CASN, 2012, p. 11).

Electronic Health Record (EHR). A record available electronically to authorized health care providers and the individual anywhere, anytime in support of high quality care. The record provides each individual in Canada with a secure and private lifetime record of their key health history and care within the health system (CASN, 2012, p. 13).

Electronic Medical Record (EMR). A record specific to a clinician's (e.g. physician) practice or organization. It is the record that clinicians maintain on their own patients, and which detail demographics, medical and drug history, and diagnostic information such as laboratory results and findings from diagnostic imaging. It is often integrated with other software that manages activities such as billing and scheduling (CASN, 2012, p. 13).

Health Information Systems (HIS). A combination of vital and health statistical data from multiple sources, used to derive information and make decisions about the health needs, health resources, costs, use, and outcome of health care (CASN, 2012, p. 13).

Lavatto (2014) sums up the leadership role in nursing, and describes a leader as a powerful person who controls or influences what other people do. Much has been written about how nurses have positively affected the quality of care for patients but little has been said in the literature about their influence in matters concerning patient information privacy and security. To learn from the nurses what latent, potential, or implied influences nurses have or could exert in the patient information privacy was of interest to this study.

2.8 Gaps in Literature

Of interest and yet a fundamental truth is that, “achieving privacy in healthcare is not a destination but a journey with a crucial mission of achieving the most appropriate balance between access to patient records and their right to privacy” (Parks et al., 2011, p. 11). These authors concluded that research to date shows a dominant reactive approach to privacy with high level solutions that do not address the operational aspects of privacy measures and effectiveness. One pragmatic and proactive approach to redressing this reported reactive and high level solutions is to directly engage significant groups who affect and are affected by patient information privacy. An exploratory study such as this, is an important first step toward understanding the nurse’s concerns, perceptions, understanding, and other operational issues that confront their daily practice involving patient information privacy.

Given that medical data disclosure is the second highest reported breaches, it is imperative to understand both information privacy and its context in healthcare (Parks et al., 2011). Parks et al. have suggested that future research should focus on the impact of information privacy measures on operational aspects of privacy measures, effectiveness, as well as answering how and what tools organizations can use to test and measure that they achieve maximum

privacy without impeding business operations. Nurses constitute a tremendous repository of knowledge, experience, ideas, and opinions for developing such metrics. Their ability to influence the patient information privacy process cannot be underestimated. Their involvement in this process to date has been minimal.

Several studies have been conducted in information privacy and security in health care. In most of these studies, opinions, perceptions, and thinking of information executives such as chief information officers, chief privacy officers, chief medical information officers (Parks et al., 2011) and other healthcare workers have been sought. Information privacy studies using empirical data is almost absent for nurses. Nurse, the largest group of healthcare providers (Kent-Wilkinson, 2008) are directly affected by information privacy. Other authors (Kotulic & Clark, 2004; Parks et al., 2011) have also commented that these areas are under researched perhaps as a result of unwillingness of organizations to share information and statistics about their practices.

I was interested to learn what nurses have to say about their anxieties and aggravations regarding changes to long established processes, increased dependence on computer systems, eroded capacity for decision making, and perceived increases in levels of accountability for clinicians in matters concerning patient information privacy. The literature is almost silent about this. As was demonstrated under the health records breaches section, significant number of breaches involving nurses have been reported in the media. What appears to be missing is some kind of suggestions of what may be the cause of such breaches, based on empirical data.

Conversations with nurses by way of semi-structured interviews may not have provided exact answers to the causes of the breaches, but clues to areas that may need further research to gain better understanding.

CHAPTER III – METHODOLOGY

This section outlines the worldview that was the background for the approach used in this research. The methodological approach used is also described in some detail here.

3.1 Worldview

The worldview I brought into this study was ontologically shaped by the philosophy that reality exists regardless of a human observer and the belief that reality is constructed in the mind of the observer. The questions I have repeatedly asked myself are “how are nurses “being” in their world of patient information privacy and security compliance, and what is their reality in this world”? How is this reality constructed? My ontological assumption followed the school of thought that posits that social reality is locally and specifically constructed by humans through their actions and interactions (Guba & Lincoln, 1994).

The ontological perspective I had was that of a relativist. I agree with Darlaston-Jones (2007) that the realist belief that there is a single objectively true characterization of reality reduces the individual to the status of a passive receptacle. Ashworth (2003), as cited by Darlaton-Jones (2007), has suggested that with this kind of thinking, there is little notion of the person as the perceiver of his or her world and even less thought seems to be afforded to the possibility of the person as a conceiver or constructor of his or her world. The tenets of relativism including the assumption that social reality is seen by multiple people and that multiple people interpret events differently leaving multiple perspectives of an incident, are appealing.

Epistemologically, my orientation was that discovery happens as an investigation proceeds, and shared with Orlikowski and Baroudi (1991) that understanding social reality required understanding how practices and meanings are formed and informed by the language and tacit norms shared by humans working towards some shared goal. I would rather make meaning of people's experiences than impute some distant inclinations.

3.2 Approach

Qualitative research method was used for this study. This method was appropriate for the study, as very little was known about the research topic (Richards & Morse, 2013). Also, the phenomenon, "nurses' experience" is not quantifiable and can best be measured qualitatively. Experience in the context of my study was; "the actual living through an event... the real life as contrasted with the ideal or imaginary ... The sum total of the conscious events which compose an individual life" (Erlich, 2008, p. 1126). Richards and Morse (2013) suggested that for broad and complex studies such as what I was proposing to do, qualitative methods work better. They can capture implicit meanings and possibly reveal information that the participants themselves may not be aware of.

3.2.1 Interpretive Description (ID)

My worldview as expressed previously naturally led me to an interpretive approach to the proposed study. According to Walsham (2006), interpretive methods of research start from the position that our knowledge of reality is a social construction of human actors. Walsham (2006) threw more light on the essence of interpretive research with a quote from Geertz (1973); "what we call our data are really our own constructions of other people's constructions of what they

and their compatriots are up to” (p. 9). The interpretive method is more interested in interpreting deeper meaning in discourse represented in a collection of personal narratives or observed behavior or activities. Thorne (2008) indicated that interpretive description is a qualitative research approach that requires an integrity of purpose deriving from two sources; an actual practice goal, and an understanding of what we do and don’t know on the basis of the available empirical evidence.

In an earlier publication, Thorne et al. (2004) stated that the foundation of interpretive description (ID) is the smaller scale qualitative investigation of a clinical phenomenon of interest to the discipline for the purpose of capturing themes and patterns within subjective perceptions and generating an interpretive description capable of informing clinical understanding. These authors added that such studies often build upon relatively small samples, using such data collection methods as interviews, participant observation and documentary analysis to articulate a coherent and meaningful account of the experiential knowledge that such methods render accessible. Same authors add that interpretive description departs from traditional qualitative descriptive approaches in that it assumes that investigators are rarely satisfied with description alone and are always exploring meanings and explanations that may yield application implications, an endeavor the researcher in this study is seeking to achieve.

Thorne (2016) proposes that in the end, ID could produce actionable information for practitioners as opposed to developing some remote theory with limited practical applications.

This study also meets the moral defensibility that the ID qualitative method advocates. Interpretive description has been used quite extensively in the healthcare industry and has been around for a while. As Thorne (2016) put it, ID is a strategy for excavating, illuminating,

articulating, and disseminating the kind of knowledge that disciplines with an application mandate tend to need in order to enact their mandate. She goes on to suggest the robustness of ID to handle complex and messy problems that demand multiplicity of insights, perspectives, and approaches used together within dynamic contexts. According to Thorne, ID sits between the spectrum of factual material and social construction to build meaningful and relevant understandings of the ideas that are of central importance to the applied disciplines.

For me, it was most interesting to learn what nurses did or didn't do, liked or didn't like, wanted or didn't want, perceived or didn't perceive, knew or didn't know, as they complied with patient information privacy and security mandates, and to find a "tool" like interpretive description that will help do exactly that.

3.2.2 Other Approaches

There were many qualitative approaches to choose from. The choice of which approach a researcher uses is often driven by the approach's fit with research purpose and/or research question. The approach I chose to use for my research was inductive thematic analysis (ITA), sometimes also referred to as general inductive thematic analysis. Inductive research approaches are often used for the purposes of condensing raw textual data into brief summary formats, establish clear links between the evaluation or research objectives and the summary findings derived from the raw data, and ultimately develop a framework of the underlying structure of experiences or processes that are evident in the raw data (Thomas, 2006).

The inductive approach is suited to analyzing data with little or no predetermined theory, structure or framework, and uses the actual data itself to derive the structure of analysis (Burnard et al., 2008). The authors also consider the inductive approach to be comprehensive. According

to Guest et al. (2013), ITA is probably the most commonly used qualitative data analysis method employed in social, behavioral, and health sciences. All the attributes of the inductive thematic approach fitted very well with my intended study. Clarke and Braun (2013) citing Merton 1975 have reported that thematic analysis in general was first named as an approach in the 1970s. Guest and colleagues (2012) have stated that the ITA process consists of reading through textual data, identifying themes in the data, coding those themes, and interpreting the structure and content of themes.

In terms of its methodological soundness, ITA shares a lot of similarities with the commonly used grounded theory (GT) and so are often discussed together in the literature. Grounded theory has in fact been described as a type of ITA, which draws on inductive analytic methods just as GT does. The approach requires free-flowing data, and is associated with in-depth interview and focus group (Guest et al., 2012). Corbin and Strauss (2008) reiterated that, GT as developed by Glaser and Strauss (1967) is a set of iterative techniques designed to identify categories and concepts within text that are then linked into formal theoretical models. Guest et al. (2012) emphasize that a defining feature of GT is the “constant comparison method”. They added that the exhaustive comparison between small units of text is often not part of many inductive thematic analysis. Another difference the same authors mentioned was that the output of ITA is not necessarily a theoretical model but often, recommendations.

Data collection approaches in general inductive thematic analyses are those typical of qualitative research (in-depth interview, focus groups, etc.). Sampling and data collection procedures in ITA context can be iterative, but can also be predetermined and temporally separate from analysis. Clarke and Braun (2013) have provided a six-phase recursive process for

successfully carrying out thematic analysis. The process starts with the researcher immersing themselves in the data and becoming intimately familiar with the data. The next phase is coding, which involves generating concise labels for important features of the data of relevance to the broad research question guiding the analysis. Coding is followed by searching for themes. This third phase requires the researcher to look for coherent and meaningful patterns in the data relevant to the research question. The next phase, reviewing themes, involves checking that the themes ‘work’ in relation to both the coded extracts and the full data-set. The fifth phase, defining and naming themes, requires the researcher to conduct and write a detailed analysis of each theme. In the final phase, writing-up, the researcher weaves together the analytic narrative and data extracts to tell the reader a coherent and persuasive story about the data, and contextualizes it in relation to existing literature.

Thematic analysis in general, and ITA specifically, has many benefits (strengths). Clarke and Braun (2013) have stated that it is relatively easy to learn and use, an opinion expressed by Burnard et al. (2008) as well. They also see thematic analysis as theoretically flexible since the search for, and examination of partnering across language does not require adherence to any particular theory of language, or explanatory meaning framework for human beings’ experiences and practices. In their opinion, this flexibility makes thematic analysis applicable within a range of theoretical frameworks. This theoretical independence leads to another benefit. Thematic analysis can be learned without some of the potentially overwhelming theoretical knowledge required for many other qualitative approaches. Clarke and Braun (2013) have also commented that thematic analysis works with a wide range of research questions including those that investigate people’s experiences and understandings. Other benefits mentioned were that the

approach could be used to analyze different types of data (focus group, interviews, secondary sources, etc.), could handle large or small data sets, and could be applied to data-driven or theory-driven analyses.

Although efficient and defendable, the general inductive approach is not as strong as some other analytic strategies for theory or model development (Thomas, 2006). Other weaknesses are those usually typical of qualitative analysis. Braun and Clarke (2006) caution against improper use of the thematic analysis approach. They mention failure to actually analyze the data at all, using the data collection questions as the “themes” that are reported, weak and unconvincing analysis, a mismatch between the data and the analytic claims that are made about it, a mismatch between theory and analytic claims, or between the research questions and the form of thematic analysis used, as well as failure to spell out theoretical assumptions or clarify how the analysis was undertaken as issues a good analysis should guard against.

As mentioned earlier, inductive thematic approach to research has been used extensively (Backet & Davison, 1995; Elliot & Gillie, 1998; Jain & Ogden, 1999; Kerse et al., 2004; Marshall, 1999; Stolee et al., 1999). Although there is a dearth of research in patient information privacy and security specifically using the inductive thematic analysis approach, a number of the authors mentioned above have used the approach to study various experiences (similar to my study) in the healthcare sector.

3.3 Conceptual Framework

Conceptual framework has been variously defined. Jabareen (2009) defined conceptual framework as a network of interlinked concepts that together provide a comprehensive understanding of a phenomenon or phenomena. He added that the methodological assumptions

of a conceptual framework relate to the process of building the conceptual framework and assessing what it can tell us about the “real” world. Jabareen (2009) suggested that a conceptual framework consists of defining component concepts. He explained that the concepts that constitute a conceptual framework support one another, articulate their respective phenomena, and establish a framework-specific philosophy. The search for theoretical understanding and its translation into meaningful practice is what is done when developing a conceptual research framework.

In this section, the main phenomenon that was the subject of the conceptual framework was “the experiences of nurses with regard to patient information privacy and security”. In order to fully understand the conceptual framework and its working, the concepts or components that make up the framework have been briefly described. Subsequently, the relationships between the components have been described in the conceptual framework development process. An attempt has also been made to piece the concepts together into a coherent whole.

3.3.1 Components of the Conceptual Framework

The core components of the conceptual framework are “experience”, “patient information”, “nurse” and “privacy”. Other components include the social and legal environments that surround nursing practice. The concepts are discussed next.

3.3.1.1 Experience. The word “experience” often denotes involvement in, participation in, observation of, and awareness of. Experience is also sometimes taken to mean an encounter, or to undergo an event or occurrence. In summary, experience is;

The actual living through an event... the real life as contrasted with the ideal or imaginary ... The sum total of the conscious events which compose an individual life
(Erlich, 2008, p. 1126)

In the development of the conceptual framework, the meaning of experience was broadened to include its everyday denotation and philosophical sense of the word. This ensured that all of a RN's experiences (feelings, thoughts, reflections, ideas, suggestions, perception, etc.) were captured during the study.

3.3.1.2 Registered Nurse. RNs have been educated to think critically, and solve all kinds of problems many of which may be unanticipated. In dealing with the issues they face on a daily basis, RNs may be constantly attempting to interpret and follow the law, and calling on their personal moral values in the context of their existing *Code of Ethics* (CNA, 2008, 2017). They also exercise professional experience and skills to make "judgment calls". In addition, privacy and security decisions are often not made in isolation but part of a complex mix that in some cases might make the difference between life and death.

The registered nurse's scope of practice is specifically outlined in *the Registered Nurses' Act*, 1988 (Statutes of Saskatchewan, 1988). The Registered Nurses Association of Ontario (RNAO, 2007b) has stated that professionalism requires that RNs in all roles demonstrate knowledge, spirit of enquiry, accountability, autonomy, advocacy, innovation and visionary, collegiality and collaboration, and ethics and values.

The Royal College of Nursing (RCN, 2003) has provided a definition of nursing which it claims could be used for developing policy and legislation. The RCN defined nursing as the use of clinical judgment in the provision of care to enable people to improve, maintain, or recover

health, to cope with health problems, and to achieve the best possible quality of life, whatever their disease or disability, until death. They pointed out that the definitions of nursing are sometimes implicit and sometimes explicit of codes of ethics specifications of the scope of nursing practice, and educational curricula (RCN, 2003). Following the discussion above, of what the registered nurse is, it could be surmised that this individual has been prepared to take control of situations, be decisive, and capable of handling all manner of nursing practice nuances, including matters concerning patient information privacy and security.

3.3.2 Development of the Conceptual Framework

The conceptual framework brings together the core concepts or components of what constitutes a RN's patient information privacy and security experience. The framework depicts the complex relationships among the core concepts and nursing practice environmental factors that act together to define the RN's overall patient information privacy and security experiences.

Nurses come into nursing practice with their own understanding of privacy and patient information, perhaps from a non-nurse perspective. The perspective they bring may have been shaped by past experiences and previous formal or informal education. In their pre-nursing states, their roles may have primarily been that of a patient, with some expectations of how their personal information needed to be handled. The past experiences, whether positive or negative, are likely to affect future behaviors. When this individual becomes a nursing student, his or her nursing education influences perceptions, beliefs, meanings, and values in patient information privacy.

While some preconceived ideas may be unlearned and even eradicated in the education process, others may persist well into practice after graduation and registration. Also, while a

student, new ideas and perceptions of privacy and security may be formed as part of the learning process. The residual notions held onto, when the student has become a RN could impact his or her decision-making process in patient information privacy and security. Although well-educated and competent, the influence of such tacit knowledge and understanding in decision making can be real for some nurses.

RNs collect, store, and disseminate patient information of all kinds as described under the patient information concept section, above. RNs need to decide what information to collect, how much of the information to collect, and how to store and/or disseminate such information while exercising due care. Patient information handling could constitute a complex set of activities that present their own challenges. Typically, patient information flow appears to begin with the patient supplying personal information not already captured in the healthcare information systems to the nurse who would use such information for clinical or administrative decision making. Often, the information flow does not follow a linear and predictable pattern as suggested here.

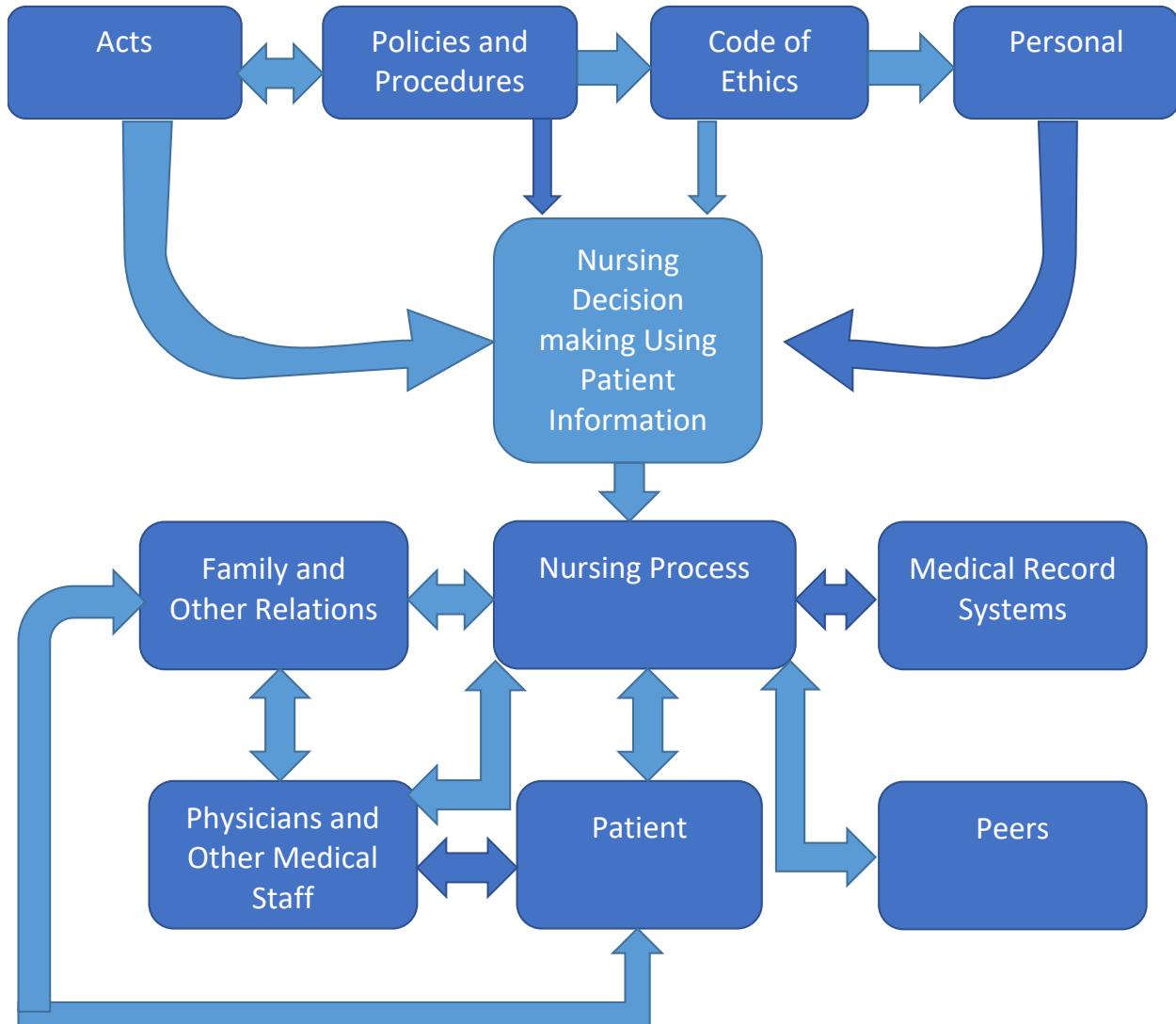
In some cases, in order to make informed decisions, patient information has travelled not only along acceptable channels of communication, but has also found its way to social media. Spector and Kappel (2012) have cited several such breaches. Social media consultation by nurses have become such a common place that, some nursing associations have developed guidelines for their proper use (Nurses Association of New Brunswick, 2012). Several variations of patient information flows that have serious consequences for privacy and security may exist in the untold stories of nurses. Thus, patient information in the hands of a nurse who needs to make informed decisions could make for interesting experiences.

A RN's patient information privacy and security experiences derive from personal observations and interactions with patients, patients' families and relations, peers in the same unit of practice, physicians, and other medical staff. Observations and interactions also occur with medical record systems, whether paper or electronic. Another important set of objects of the nurse's interaction are the Acts, policies and procedures, codes of ethics, best practices, and other relevant guidelines. Of note is that a RN's patient information privacy and security experience often occurs as he or she assumes the nursing role. The nursing process itself provides another context for varied experiences. Beginning with assessment, through diagnoses, planning, implementation, and evaluation (Semachew, 2018), elements of information collection and sharing could generate privacy and security experiences. The figure below is a simplified illustration of the interaction between the components that generate a nurse's patient information privacy and security experiences.

Figure 3.1:

Interactions Between Components of Conceptual Framework That Generate a Nurse's Patient Information Privacy and Security Experiences

Conceptual Framework for Patient Information Flows and Influences



The conceptual framework described above provided some indications of the nature of the context for nurses' experiences. The conceptual framework was not an attempt to explain why nurses experienced what they did, neither was it designed to elucidate how those experiences occurred. The primary purpose of the framework was to set the boundaries for

asking the appropriate research question, and for understanding nurses' patient information privacy and security experiences as they were told.

In the simple framework illustrated above, a patient provides information to the nurse, with the nurse being aware of the implicit patient-nurse confidentiality. Patient information may also be coming from the patient's family, information the patient may have supplied to the family. The nurse may share such information with relevant physicians. Patient information may also be stored and retrieved from medical record systems. The RN makes critical clinical and administrative decisions using patient information. The decision processes are influenced by the existing legal context, ethical codes of conduct, and personal beliefs.

As nurses tell their individual stories of their encounters and interactions within the framework described above, the researcher together with the participants of the research would co-construct a thematic portrait of concerns, understanding, beliefs, cognitions, interpretations, and even unanticipated findings that nurses bring to patient information privacy and security.

3.4 Research Design

This section describes the systematic plan for the qualitative research study. Specifically, it addresses the setting for the research, sampling strategy and procedures, and data collection procedures. Also addressed in this section is the rigor of the research, including data trustworthiness. Data analysis and dissemination of findings, as well as ethical considerations are included in this section.

3.4.1 Setting for the Study

The primary method of data collection, which will be addressed later in more detail, is through interviewing. The ideal setting for interviewing was a comfortable room in the hospital

to take advantage of recent experiences (recall). The best time for interviewing was planned for when the participant has had time to unwind and was relaxed. The location was one most preferred by the participant with minimum distraction. The reason a hospital location was preferred for the study was that hospitals handle a high volume of patient traffic and are likely to provide a representative variety of nursing experiences. The study was restricted to two hospitals, one each in the provinces of AB and SK. This choice was based primarily on logistical feasibility. Interviews were conducted individually.

Depending on if the initial interviews were producing desired results, plans were made for interviewing small groups at a location each group member agreed on (Richards, 2009). The small groups would be made up of 3-4 individuals. Most participants indicated that they were more comfortable sharing their experiences in a one-on-one setting with just the interviewer. Regarding the time of day for the interview, any time that met the participant's convenience was acceptable.

3.4.2 Sampling Procedure/Strategy

The target population was medical-surgical registered/critical care nurses in the Alberta and Saskatchewan health regions. Medical-surgical/critical care nurses were chosen for several reasons. They deal with a wide variety of patients including different age groups, different diagnoses, male and female, in essence, they capture a wide range of experiences. These nurses also handle a high number of patients and interface with a variety of other nursing units, and are actively involved in patient information handling. The context of their nursing practice provided a rich set of patient information experiences.

Participants were purposefully selected to ensure that varying years of overall nursing experiences were covered. Participants were selected from the 18-30 years, 31-40 years, 41–50 years, and over 50 years age groups, and consisted of male and female nurses. This allowed for a broad range of perspectives. Inclusion criteria for the target population was all registered nurses who currently worked or have worked in the medical-surgical/critical care unit for at least 12-24 months and could recall experiences. This duration of medical-surgical/critical care experience was chosen arbitrarily in anticipation that there will be sufficient lived experiences. Nurses not meeting the above criteria were excluded. A couple of nurses who wanted to be interviewed but did not qualify were excluded upon initial questioning. Part of the inclusion plan was that eligible nurses who during the interview process indicated by their actions or expressed any feeling of being coerced to partake in the study would be given the opportunity to back out of the interview and excluded. Fortunately, there was no such incident.

Samples were drawn from the pool of participants who had responded and agreed to an earlier invitation to participate in the study. Access to the participants was through a contact (gate keeper) at the hospital and/or nursing associations, and also through previously interviewed nurses. Gatekeepers at various hospitals and nursing associations were contacted prior to the study. A description of the purpose, objectives, significance, and eligibility criteria for participants of the study were provided to the gatekeeper. The researcher's contact information was provided as well. The gatekeeper was informed that participation was completely voluntary. The researcher and the gatekeeper then designed and wrote a notice regarding recruitment for the study that was disseminated to nurses using their existing means of communication. The notice required that interested participants contact the researcher directly. Distribution of the notice was

done as neutrally as possible to ensure that any appearance of possible coercion was removed. A letter of invitation is included as Appendix 2.

As suggested by Creswell (2014), initial sampling began with 20-30 participants. This number was divided between AB and SK. In all, twenty participants were interviewed. In Alberta, 9 participants were interviewed, of which 2 were male and 7 were female. The Saskatchewan participants consisted of 1 male and 10 females, bringing the total to 11 participants. Since the samples were from a purposively chosen population, it was believed that the samples likely enabled a better understanding of the problem and research question (Creswell, 2014). The sample size was ultimately determined at saturation, the point where no new or additional insights were discovered about categories that had emerged from simultaneous data collection, coding, and analysis.

3.4.3 Data Collection Procedures

Data collection was done using semi-structured in-depth interviews. Interviews provided in-depth information pertaining to participants' experiences and viewpoints of a particular subject (Turner, 2010). Arrangements were made with prospective interviewees to ensure that interview schedules were conducive to their personal life situations. Upon meeting with the participants, the interview began by explaining the purpose of the study to the participants and how the study might benefit them. A consent form (see Appendix 3) was given to the participants to read and sign (Richards, 2009). As described under the "Setting of the Study" section, the researcher had planned to interview together, groups of three-four participants on occasions when needed. Plans were also made to use focus groups if it was deemed necessary to use bigger groups (eight-ten) (Central Connecticut State University, 2013). Focus groups have

several advantages including their cost and time effectiveness, and allowing the researcher to draw on respondent's attitudes, feelings, beliefs, and experiences. Focus groups are particularly useful when new products and services are being developed and the organization is not sure how a particular group will react. Focus groups also have limitations. Such limitations include the inherent risk of dominant participants influencing others. The primary reason "focus groups" was not used in this study was due to the sensitive nature of the study. Some of the raw and honest responses obtained during the study were because of the one-on-one nature of the interviews. Interviewees did not have reservations as a result of the presence of certain individuals.

Although an interview guide (see Appendix 5) was used, interviewing was largely conversational, to put participants at ease. Open-ended questions were used to allow participants to tell their stories.

Data were recorded by note taking at the time of the interview and audio recorded as well. If data recording made a participant uncomfortable, the plan was to discontinue recording and participant excluded. There was no such incident. Face-to-face interviewing was important to this study as body language and expressions often communicated or insinuated feelings and attitudes that sometimes words could not do justice to. Memos were written on the field notes to provide immediate illustration of an idea (Glaser & Strauss, 1999). Interviewing started with an ice-breaker to build a relaxed atmosphere and set the stage for the subsequent questions.

Participants were compensated for their time in the form of a \$30 gift card. Individual interviews were planned for approximately 30-45 minutes and the group ones for a little longer, if they became necessary. The researcher's contact information was available to the participants through mail, email or the gate keeper prior to the scheduled interview.

Interviewees were given the opportunity to clarify any doubts they had regarding the interview. If the use of focus groups became necessary, the interviewer was aware that the number of focus group meetings depended on outcomes of previous interviews. Similarly, subsequent interviews with the same participant were only necessary if on-going data analysis revealed interesting phenomenon requiring further investigation.

Record keeping using memos was used extensively during data collection. As Richards and Morse (2013) suggested, they were used to record events observed and moods during interviews. They were used to keep record of impressions, served as reminders for things to watch for in the future, for reflection on words or phrases, and also to record ideas about an item.

The iterative nature of qualitative research process in which preliminary data analysis coincides with data collection often results in altering interview questions as the investigator learns more about the subject (Dicicco-Bloom & Crabtree, 2006). Initial questions that were not effective at eliciting the necessary information were dropped and new ones added. Following the suggestion of Dicicco-Bloom and Crabtree (2006), the interview was flexible enough to allow some digression, as such digressions were very productive as they followed the interviewee's interest and knowledge.

Jacob and Furgerson (2012) noted that when professionals interview, they ask people to share their stories. They pointed out the importance of good interview protocol and offered several guiding principles. These principles included asking the interviewee basic background questions as a way of warming up participants, beginning the interview session with easy to answer questions and progressively moving to difficult or controversial questions. The authors also suggested writing expansive questions. Such questions made interviewees say things that

you would have never thought to ask. They further advised that interviewers set up a second interview to help clarify or ask any questions missed after transcribing the interview. The guiding principles were useful in the construction of the interview guide in Appendix 5 and during the interview processes themselves.

CHAPTER IV – DATA ANALYSIS

Data collected were organized and prepared by transcribing interviews, and typing field notes. There were reviews of all data as a first step to providing a general sense of the information and to reflect on their overall meaning. Coding then began after the review. Creswell (2014) has provided an eight-step guide that was followed during coding. In order to get a sense of the whole, all transcripts were read, writing down fresh ideas as they came to mind. As I read the transcripts, I also noted and assigned level of priority depending on how interesting the transcript read. The most interesting transcripts (selected 10-15) were carefully read again to ascertain what the responses were about, and the underlying meaning. Notes were written on the transcript concerning thoughts that came to mind. A list of all topics that were noted were compiled. Similar topics were clustered together and used to make columns. The selected topics were used to characterize segments of the other text. This organizing scheme was used to see if new categories and themes emerged.

The topics were turned into categories by thoroughly describing the preliminary topics. In order to reduce the number of categories, topics that related to each other were grouped together, and diagrammatically to show interrelationships. Each category was abbreviated and alphabetized as codes. Data material belonging to each category were assembled in one place and preliminary analysis performed.

A detailed description of the participants and events has been rendered to provide perspective. Themes and categories have been presented, and findings interpreted. Data analysis occurred concurrently with data collection so that the investigator could generate an emerging

understanding about the research question(s), which in turn informed both sampling and questions being asked.

4.1 Purpose of Data Analysis

The aim of data analysis was to look for emerging ideas, categories, concepts, and themes from the data. Analysis followed a continuous and responsive interaction between data collection and analysis, as mentioned earlier. Data were coded using participant language, with the purpose of simplifying and focusing on some specific characteristics of the data (Richards & Morse, 2013). Coding helped in locating information. A commonly used approach relies on using codes from a code-book for tagging segments of text and then sorting text segments with similar content into separate categories for a final distillation into major themes (Dicicco-Bloom & Crabtree, 2006) as described before. Through the process of coding, the researcher creates and develops abstractions from the data. Coding also helped the interpretation of ideas by pointing to the data from which the idea evolved.

Data were stored on a computer, and although the software of choice was NVivo, mainly as a result of its popularity, robustness, ease of use, and compatibility with other software, this software was hardly used. Analysis was primarily manual, as the researcher wanted to be intimately immersed in data analysis. Results of data analysis will be presented by description and figures depicting discovered categories and their relationships (Creswell, 2014).

In order to clarify and justify my study, I have demonstrated in previous sections the soundness of fit of the research question, aims and the choice of methods appropriate to the research problem. Procedural rigor has been achieved through transparency in regards to the way

the study was conducted. Details of how study participants were accessed have been thoroughly described. Data collection process, recording, coding, and analysis have been explicitly accounted for, including accounts of the manner in which errors or subject refusals were dealt with. In the interpretive process, accounts of “negative” or “deviant” cases are especially important. These are explanations pertaining to data or evidence that contradicts the researchers’ overall explanatory account of the phenomena (Kitto et al., 2008). Reflexivity is where the researcher openly acknowledges and addresses the influence that the relationship among the researcher, the research topic and subjects may have on the results. Thick descriptions have been used in subsequent sections to portray the reality of participants’ lived experiences.

To establish credibility, journaling of all activities involved in the study including the amount of time planning, following up, scheduling, week end hours, and inconveniences accommodated in order to get the study going have been documented. My records and other documents have been appropriately made available for audit. Member checking was done by taking descriptions and themes back to the participants to check for accuracy (Creswell, 2014) through the nurses’ gate keeper. This meant offering the subjects interviewed the opportunity to view and amend their transcripts as a type of validity. This is important because, as Darlaston-Jones (2007) commented, it is as a result of the conversation between the respondent and the researcher that resulted in the co-construction of meaning that emerged.

I have clarified my personal biases as a result of my past observations and experiences as a patient in a hospital. When reporting my findings, it was made clear to my readers that generalizability and transferability were not the intentions of the study. This will be achieved by

explicitly stating the aforementioned, and by good description of my study population and samples used.

4.2 Ethical Considerations

Ethical issues have been addressed at various stages of the study; prior to conducting the study; beginning of the study; at data collection; data analysis; during sharing; and storing of data. The codes of conduct for AB and SK registered nurses were reviewed to ensure that processes followed during the study did not violate any of the ethical codes before the study started. Ongoing consultation of the Code of Ethics continued throughout the study. Prior to the start of the research study, a proposal was submitted to the University of Saskatchewan Review Ethics Board (REB) for approval. The researcher went through the proper approval procedures for the study sites before the study's commencement. A copy of the certificate of approval (BEH #15-331) from the University of Saskatchewan review board is included as Appendix 1.

Informed consent form outlining important considerations were provided for the participants to read and sign. A copy of the consent form is included as Appendix 2 to this proposal. The general purpose of the study and how data will be used has been discussed with the participants to clarify lingering doubts or suspicions in the minds of participants. This was also to assure participants that their information will be protected and not used in any adversarial manner. While the study was ongoing, efforts were made to respect norms, traditions, and established cultures that the nurses may have.

During data collection, each participant was treated with the same level of courtesy and respect. The researcher continued to seek participant permission to do anything not anticipated before data collection began. Participants were encouraged to let the researcher know

immediately if they perceived any form of exploitation at the time of interview or any other time.

Information that would be harmful to a participant were not collected. The privacy of participants was explicitly conveyed to them not only before the study began but also during interviewing for reassurance. For example, fictitious names were used when making reference to participants. Composite descriptions were also used to conceal the identity of participants.

The researcher was careful not to take sides. Discussions during analysis of data was inclusive and did not show indications of favoritism. Also, data that proved or disproved personal hypotheses that the researcher may hold were disregarded (Creswell, 2014). To uphold honesty in research, contrary as well as positive results have been disclosed. Accurate interpretation of data has been provided as well. Peer reviews and audit strategies have been used to curb the possibility of suppressing, falsifying, or inventing findings. Information that has the potential of harming a participant has not been disclosed. Data have been shared with others to allow for personal judgment regarding credibility. Raw data and other materials will be kept by the researcher for a reasonable period of time and discarded in a manner that prevents access.

This includes destroying media containing the raw data.

4.3 Dissemination of Findings

Researchers in general publish and disseminate work in many different ways. According to a report jointly published by the Research Information Network and the Joint Information System Committee (2009) in the United Kingdom, researchers are motivated by a number of interrelated factors beyond the simple desire to pass on their findings to those who may be interested in them.

These motivations include the desire to register their claim to the work they have done, and to gain peer esteem and the rewards that may flow from that.

The Alberta Institute of Health Economics (2008) used the term “knowledge translation” in place of dissemination of findings. They defined knowledge translation as ensuring that stakeholders are aware of and use research evidence to inform their health and health care decision-making. The Institute of Health Economics added that the definition recognizes a wide range of stakeholders or target audiences for knowledge translation, including policy makers, professionals, patients, researchers and industry.

I subscribe to the Institute of Health Economics’ (2008) idea of knowledge translation. In my estimation, the findings of the research will be new knowledge gained. This knowledge needs to translate to action in the real-world in a practical sense, and will also add to the existing body of knowledge. The primary stakeholders for my findings are healthcare policy makers, researchers, and nursing professionals. Although the findings are not intended for direct policy decision making, it will likely shed light on specific areas in patient information privacy and security policy that need further investigation to enhance policy decision making. Nursing researchers and others interested in privacy and security research would be better informed in this important area of privacy and security of personal health records. Dissemination efforts will thus be focused on the audiences named above.

The basic procedure in reporting the results of the exploratory qualitative research study is to develop descriptions and themes from the data, and to present these descriptions and themes that convey multiple perspectives from participants and detailed descriptions of the setting or individuals (Creswell, 2014). Detailed descriptions of experiences will be provided, and that may include co-constructed meanings. Interpretation of the results of data analysis may also capture dominant themes and their underlying rationale, the inter-relationships among themes and their

meanings in light of what is known in existing literature. The report was written to clearly portray “what is going on here” in the patient information privacy and security world of the nurse. In a way, the primary goal was to describe how nurses feel, think, and behave in the context of patient information privacy and security compliance.

With the target audience in mind, nurses, I have written the findings in an organized, to the point manner. In order to make the report interesting and hold readers’ attention, only new and compelling findings will be presented. Findings will also be presented so they flow in logical progression. Conclusions and recommendations will be articulated as clearly as possible to ensure that readers know what to do with the information. If readers know what to do with the information, they are more likely to apply it. The report will not be published until multiple perspectives and feedbacks have been solicited from significant representatives of the stakeholder communities. Their input will be needed to ensure that information in the publication is correct and easy to understand. Contents of the findings will first be shared with academics in nursing education, nursing associations, and interested nursing students in SK and AB. The report has also been subjected to peer reviews by other scholars in the nursing and information privacy and security fields.

The primary media for publication of the study findings will be credible nursing journals and information privacy and security journals, and journals that focus on nursing informatics or nursing ethics. Findings could also be disseminated by presenting at notable and relevant conferences. Other useful media include policy briefs. Results of the study will not be published in press releases, flyers, posters, and brochures just for the sake of publicity.

CHAPTER V – RESULTS

The target population from which qualitative data was collected was medical-surgical and critical care registered nurses in the AB and SK health regions. In all, data were collected from twenty (9 from AB and 11 from SK) nurses through the interview process. About 540 lines of code were generated. After grouping of the lines of code, 13 initial categories were identified.

Further grouping resulted in seven themes. Two overarching themes were derived from the nurses' responses to the interview questions. These two broad themes were, "Patient Information Protection" and "Patient Information Violations (Breach)". Each of these two major themes had five contrasting (dichotomous) subthemes as to how patient information was secured or infringed upon.

In addition to the themes that emerged, the nurse participants inadvertently articulated in the data their beliefs about the meanings of the key terms, which resulted in co-constructed definitions of the key terms that related to: patient information protection, patient information privacy, patient information breach, etc.

5.1 Purpose of Research

As indicated earlier in this dissertation, the purpose of the research was to gain better understanding of the experiences of (RNs) in patient information privacy and security in the AB and SK health regions. Specific goals included capturing rich insights and concepts related to perceptions, feelings, reflections, thoughts, and even apprehension and comprehension for nurses. Such insights should hopefully lead to understanding what is important or not important to RNs, to ascertain specific implications, to provide evidence or ideas to understanding some existing behavior patterns, and to inform future research.

5.2 Demographic Statistics and Observations from the Study Participants

This section provides a description of the study participants in AB and SK. The table below provide descriptive summaries of the participants in the two provinces:

Table 5.1

Demographic Statistics of Study Participants

AB Participants

Gender	Age (Years)	No.	Ethnicity	Education RN	Years of Experience
Male (2) Female (7)	18-30	0	Caucasian (7)	RN only (4)	1-10 yrs. (3)
	31-40	5	African (1)	RN, BN/BSN/BScN (9)	11-20 yrs. (4)
	41-50	2	Asian (1)	MN (0)	21-30 yrs. (1)
	50+	2		PhD (0)	30+ yrs. (1)

SK Participants

Gender	Age (Years)	No.	Ethnicity	Education RN	Years of Experience
Male (1) Female (10)	18-30	1	Caucasian (9)	RN only (5)	1-10 yrs. (4)
	31-40	4	Asian (2)	RN, BN/BSN/BScN (10)	11-20 yrs. (5)
	41-50	4		MScN (1)	21-30 yrs. (1)
	50+	2		PhD (0)	30+ yrs. (1)

The participant demographic form is included as Appendix 4. As indicated earlier, there were twenty participants in all, from the two provinces of AB and SK. In all, there were three males and seventeen female nurses in the study. The AB participants ranged in age between thirty-one and over fifty years; in AB 5 of the participants were between the thirty-one and forty years old, therefore a bit younger as a group than those in SK. In all, the ethnic mix was predominantly

Caucasian (16) with three Asians and an African. Perhaps, the defining characteristic that was important to this study was years of nursing experience. As could be seen from the table above, there were at rich combination of years of nursing experience. In all, there were thirteen nurses with more than ten years of nursing experience. Regarding the differences in years of nursing experience between the two provinces, the differences were negligible, although the SK nurses were slightly more experienced. In terms of educational background, none of the nurses that were interviewed had below a bachelor's degree.

During the study, it was apparent that most nurses were not that familiar with the actual patient information privacy and security Acts. They however appeared to be conversant with the unit policies, many of which were derived from the Acts. The older nurses in both provinces who had worked at different places provided some insights regarding paper and electronic records, and often defended their belief that paper records may be more secure than electronic records.

Among the nurses, particularly the more experienced ones, there were no disputes about finding there was more experience with electronic records in AB than in SK. Older regulatory compliance issues, according to the nurses, were more likely to be in SK than AB. There was some indication that the nurses in SK were more concerned about the privacy infrastructure than their counterparts in AB. Participants in AB were more optimistic regarding resource availability including those for securing patient information privacy than in SK. According to a nurse in SK, the nurses felt that the healthcare system was being ignored and that the breaches are occurring so the nurses can get the attention they need.

5.3 Definitions Emerging from the Data

Early in the data analysis it became evident that participants had their own interpretations of the key terms that influenced their practice with regard to patient information privacy, security and breach etc. As the participants (nurses) described, categorized and contextualized each important term, it became evident that there were significant concepts associated with each one in their interpretations.

Table 5.2

Definitions Beginning to be Interpreted or Co-Constructed from the Data

Definitions Co-constructed from Data
<ul style="list-style-type: none">• Patient Information Protection (PIP)• Patient Information Privacy (PIP)• Patient Information Safety• Patient Information Security• Patient Information Breach (Infractions/Violation)<ul style="list-style-type: none">• Nurse-patient relationship “trust”
Definitions Co-constructed from Data
<p style="text-align: center;">Patient Information Protection</p> <ul style="list-style-type: none">• Nurse participants clearly stated that being intentional about respecting the patient’s information was necessary for protecting it. <p style="text-align: center;">Patient Information Privacy</p> <ul style="list-style-type: none">• ‘Privacy’ was a word often used synonymously with ‘protection’ of patient information.• Nurse participants believed that patient information privacy was a professional obligation. and needed to be treated as a duty, and that the nurse is a custodian of the patient’s information.• Some interviewees believed that a person’s personal information belongs to that person.• According to some nurse participants, discreetness in accessing patient information is a tenet of privacy, and for the nurse, privacy is a matter of due diligence.<ul style="list-style-type: none">• To the nurse privacy means not accessing information not meant for you.• Other meanings associated with privacy were, assurance of confidentiality as well as patient consent, assurance that what is shared is not revealed to other people.<ul style="list-style-type: none">• The nurses indicated that privacy has to do with “need to know”.• There was the suggestion that privacy could entail divulging a level of patient information but leaving out details.

- Privacy also meant safety of information from outside parties.
- The meaning of privacy was contextualized to reveal the level of importance.
- There was also the perception that privacy is unrealistic, given the current working conditions.

Patient Information Safety

- ‘Privacy’ also meant ‘safety’ of information from outside parties.

Patient Information Security

- The meaning of patient information security was often subsumed by the definition of privacy. This therefore meant that the terms “privacy” and “security” were used interchangeably by the nurses.

Patient Information Breach

- The nurse participants categorized breaches as being intentional or unintentional, as circumstances could lead to accidental divulge of information.
- *Intentional breaches* the nurse respondents talked about included: nurses accessing their own health records; looking at patient information not needed to provide care; looking at information, or sharing information you are not supposed to; accessing patient information of a neighbour or another nurses’ records.
- A respondent mentioned that intentional breaches may simply be as a result of lack of morality, prying, or malicious intent.
- *Unintentional breaches* the nurse respondents mentioned were: asking and being told about patients not in their care, but due to the “interesting” nature of the patient’s case;

Nurse-patient relationship “trust”

- The nurses acknowledged that patients trusted nurses with their personal information, regardless of what form it was in.
- There was the supposition that nurses are in a position of assumed trust, and that patients share freely with nurses as a result of trust.
- The nurses believed that patient information privacy led to information protection practices and built trust between patient and nurse. Some even went as far as alluding that privacy was an established trust between the nurse and patient.
- The thought of the possibility of punishment for breaking trust was also entertained by nurses.

5.4 Primary Research Question

As a result of the exploratory nature of the study, the primary research question was broadly stated as, “what are the experiences of medical-surgical and critical care registered nurses as they comply with the Alberta *HIA* (Government of AB, 2020a, 2020b) and the SK

HIPAA, (Government of SK, 2020a, 2020b) in their day-to-day nursing practices in a hospital?”

Other relevant questions related to the primary research question are “what meanings do nurses bring to patient information privacy and security practices?”, “are nurses concerned about the expectations mandated by Health Information Acts?”, “how adequate is the preparation nurses receive in the area of regulatory compliance?”

5.5 Broad Themes and Subthemes (Dichotomous Themes)

The two main over-arching themes evident were (A) Protection of Patient Information (intentional v. unintentional measures to secure; regulatory compliance v. interpretation of regulatory compliance; protection initiatives v. unprotected; expectations v. realities), and (B) violations or breaches to Patient Information (intentional v. unintentional breach/infringe; attitude towards breach v. causes of breach; actions v. inaction).

Each of the overarching themes had contrasting (dichotomous) subthemes or factors that either “secured” or “breached” patient information, in terms of (1) Access to Patient Information (open or accessible v. restricted access; too much v. too little information; sharing v. protecting of information); (2) Education of Patient Information (awareness v. ignorance; knowledge v. insufficient knowledge; education v. lack of education); (3) Nursing Practice (professional obligations v. human nature; challenges v. consequences; safe v. unsafe practices; trust v. mistrust); (4) Electronic Records and/or Paper Records (secure v. vulnerable; benefits v. pitfalls); and, (5) AB and SK Health Regions (similarities v. differences in AB and SK; urban v. rural; resources v. limited resources).

Table 5.3:

Themes and Sub Themes

Two Over-Arching Themes:
(A) Protection of Patient Information (Privacy) <ul style="list-style-type: none"> intentional v. unintentional measures to secure; regulatory compliance v. interpretation of regulatory compliance; <ul style="list-style-type: none"> protection initiatives v. unprotected; expectations v. realities.
(B) Violation of Patient Information (Breach) <ul style="list-style-type: none"> intentional v. unintentional breach/infringement; attitude towards breach v. causes of breach; <ul style="list-style-type: none"> actions v. inaction.
Sub Themes (dichotomous) <ul style="list-style-type: none"> Each of the overarching themes had contrasting (dichotomous) subthemes or factors that either “secured” or “breached” patient information, in terms of:
(C) Access to Patient Information <ul style="list-style-type: none"> accessible (open) v. restricted access to information; sharing information v. protecting information. (D) Education of Patient Information <ul style="list-style-type: none"> awareness v. unaware; adequate knowledge v. insufficient knowledge; <ul style="list-style-type: none"> education v. lack of education. (E) Nursing Practice <ul style="list-style-type: none"> professional obligations v. human nature; <ul style="list-style-type: none"> challenges v. consequences; safe v. unsafe practices; trust v. mistrust; (F) Electronic Records and/or Paper Records <ul style="list-style-type: none"> secure v. vulnerable; benefits v. pitfalls. (G) AB and SK Health Regions <ul style="list-style-type: none"> similarities v. differences in AB and SK; <ul style="list-style-type: none"> urban v. rural; resources v. limited resources

This section presents details on each of the themes derived from the data collected from the interviewees. Examples of data are provided where necessary.

5.6 Theme A - Patient Information Protection

Patient information protection as used or implied by the respondents had a wide range of meanings. In one sense, the phrase was used to connote actions or lack of action that lead to the vulnerability of patient information. Nurses were apprehensive of patient information left open on computer screens while getting for example, coffee. Behaviours of this nature were a struggle for some who perceived behaviours as carelessness. Adequacy of monitoring in light of current information sharing methods such as faxes and email was a concern. A respondent made a statement that captured the essence of this concern. She said, “... a nurse who has worked I think for eleven years in different hospitals, who had always been going into different patients accounts, why or how she wasn’t caught all these years beats me though ...” (REC012 CAL AB: L8-11). Another important concern was failure to log out after use of generic systems. A nurse described this in her own words as follows, “... some people don’t always sign off on the system and they leave the cart in the hallway when they go do something, so patient information is easily accessed...” (REC 20 CAL AB: Pg3-L1-3).

5.6.1 Protection Initiatives

The nurses mentioned several protection initiatives in place that they appreciated. One such initiative was the signing of affidavit not to engage in certain unsafe practices. Among the steps that were taken to protect patient information were filtering calls to protect the patient’s privacy, audits to see who is accessing what information and whether that information was pertinent to what they did, and in some cases, lying to conceal a patient’s identity. As a nurse emphatically stated, “...then it’s easy for us to say we don’t know who you’re talking about. There’s nobody on this unit with that name ...” (REC017-P-CAL-AB: Pg4-L24-25). There was

also indication that some patients came in as “confidential patients” with no name and no charts on the board, as for example, a patient admitted as a result of domestic abuse. Steps (use of passwords, not allowing names on worksheets and finding alternatives to identifying patients) were taken to protect such patients.

5.6.1.1 Intentional v. Unintentional. Nurse participants clearly stated that being intentional about respecting the patient’s information was necessary for protecting it. As one nurse emphatically put it, “... as a custodian of care services, I need to always honor and respect a person’s privacy...” (REC012 RD AB: p. 2, L16-17). Some interviewees believed that a person’s personal information is their own and needed to be respected, and as a respondent reiterated, “... as a clinician in healthcare, I’ve always been conscientious of the fact that I’m dealing with people, and their information is, from my perspective, to be respected, and not to be shared with others unless absolutely necessary as part of their treatment plan, their care...” (REC012 RD AB: L10-13).

5.6.1.1.1 Respect. Respect for patient information privacy was mentioned by a number of nurses. Privacy meant to respect the patient’s information unless it needs to be part of a treatment plan. Nurse participants believed that patient information privacy needed to be treated as a duty, and that the nurse is a custodian of the patient’s information. One nurse said that “... so it’s extremely important in terms of a topic, and what it means to me is that, as a custodian of care services, I need to always honor and respect a person’s privacy...” (REC012 RD HRIS AB: L15-17). Some nurses indicated that maintaining the privacy of patient information is a professional obligation. According to them, nurses need to follow rules as a matter of ethical duty. Some nurse participants also mentioned that discreetness in accessing patient information is a tenet of

privacy, and for the nurse, privacy is a matter of due diligence. The participant put it this way, “... whether it’s necessary to be shared with others, I have the due diligence to consider the impact of whether or not it’s going to be of value to that person’s care...” (REC012 RD CHRIS AB: L13-15).

To the nurse, privacy means not accessing information not meant for you and that, privacy is a nurse’s obligation and value. Other meanings associated with privacy were, assurance of confidentiality as well as patient consent, assurance that what is shared is not revealed to other people. The nurses indicated that privacy has to do with “need to know”, with some asking the question, “who needs to know?” In response to a question about “need to know”, here is what the interviewee had to say; “...and as we talk about all the time, like it’s a need to know basis, but who is in that need to know...” (REC004 SK: L21-22). There was the suggestion that privacy could entail divulging a level of patient information but leaving out details. Privacy is now more nebulous – even the idea that electronic record keeping could be used to preserve privacy.

5.6.1.1.2 Safety. Privacy also meant safety of information from outside parties. The interviewees pointed out that privacy initiatives should consider data transmission, proximity of other patients when patient information is being shared, locking the unused workstations, physical placement of nursing stations, with the use of dry-erase boards considered to be privacy concerns. Reporting to next shift and bedside reporting in shared rooms were privacy concerns as well. There was also the perception that privacy is unrealistic, given the current working conditions. There was the belief that it is never going to be completely private or safe. The idea of privacy for comfort was also mentioned – a new idea. A nurse elaborating on this idea

commented, “... and also as a nurse that kind of makes me feel more at ease knowing that my patients feel potentially more comfortable, secure, and safe about their information if that’s a big concern ...” (REC002S:L23-25). Another nurse referred to “privacy for comfort” as ”...privacy so they can sleep. Privacy for comfort, so to speak right?” (REC021 SK: L5-6).

5.6.1.2 Expectations v. Realities. Patient information privacy and its expectations appeared to be well understood by nurses and taken seriously. The nurses were in agreement with regulatory compliance, but there was a noteworthy comment that attitudes to regulatory compliance may also depend on what type of day the nurse is having. Regarding “privacy infrastructure” initiatives, some respondents indicated that private rooms are gaining grounds with new facilities. In some cases, privacy consultants are available to answer questions.

The realities of day-to-day nursing practices are that nurses are aware of the incessant posting of what one nurse calls “non-descriptive” content to the internet and the fact that nurses are generally apprehensive of this. In a respondent’s own words, “... I’ve heard of that as well, of people posting supposed non-descriptive things, but the reality is that it’s still putting it out on the internet, and it’s personal information. And so, it was not ok before Facebook to post it on the internet, it’s not ok to do it now...” (REC020 AB: L28-31). Nurses were also realizing more and more, the need to be careful about what they say. One nurse expressed this realization after overhearing fellow nurses talk about a patient this way, “... can be a challenge and then you know realizing that I need to be careful of what I say because you never know who is in the room with you that could potentially know a person because, you know, what you say can always get out and ...” (REC002 SK: L27-30). Some also commented on the reality of when it came to divulging a patient’s information by saying that, “... a lot of it just depends on the certain

situation, and also the type of day that you're having, um like, a lot of it, if you're just run off your feet and you've got something really critical to get done, and then somebody asks you to do something quickly, you may just say it without even you know, realizing... you're human so you're going to sometimes have little slips here and there..." (REC004 SK: L27-31).

5.6.1.3 Regulatory Compliance v. Interpretation. Another area that received attention when it came to patient information protection was regulatory compliance. The ultimate purpose of regulatory compliance in the area of patient information is to protect patient information.

Regulatory compliance provides the assurance that patient information privacy rules are followed. The nurses, however, reiterated that at times, different nurses may interpret compliance regulations differently. In a nurse's own words, "... I feel that where the fault actually lies is not with regulations. It's with how people interpret them into what people do, in their day to day practice..." (REC009-M-RD-AB: Pg3-L5-6).

One interviewee pointed out that regulations were not the problem, interpretation sometimes was. Other times, the language the regulations were written in could be a concern. There was the thinking that the regulations were not followed due to lack of knowledge. Some nurses felt that privacy regulations were cumbersome and in the way. Some suggested that nurses dislike bureaucracy and had strong preference for common sense. They added that some conform to regulations more out of fear than personal conviction. Yet, there were others who thought regulations are not impediments but imperative. The direct words of the respondent were, "... there's processes in place that can actually be utilized, whether it be for disciplinary actions or others, to ensure that the integrity of people's information is only used for the right reasons. So regulation is imperative..." (REC012 RD AB: L8-10). This was strongly expressed

by other nurses in terms such as, "...I think the Alberta Health Service, the provincial, the federal and professional regulations are critical to maintain privacy of information..." (REC008 RD AB: L26-27).

5.7 Theme B - Patient Information Breach

The nurse participants categorized breaches as being intentional or unintentional, as circumstances could lead to accidental divulge of information. The nurse participants also shared their perspectives on attitudes towards breaches, and what they thought were some of the causes of breaches.

5.7.1 Intentional v. Unintentional

The intentional breaches respondents talked about included nurses accessing their own health records. According to the nurses, a breach could also be checking on patient information that does not help to provide care. Some nurses further indicated that a breach is looking at information, or sharing information you are not supposed to. In other circumstances, nurses would access their neighbour's or other nurses' records probably as a result of concern for these individuals or just prying. A respondent mentioned that breaches may simply be as a result of lack of morality. Patient records were also breached as nurses shared unusual experiences on Facebook with their friends and family. Breaches occurring due to malicious intent was suggested as well. On other occasions, breaches had occurred just because the patients happened to be celebrities. In some cases, breaches happened to portray emotional feelings and to bring about change, especially when a nurse feels strongly about an issue and would like to draw public attention to it. A nurse said, "... because I think people put this information on Facebook,

or yeah they feel like they are trying to get more help or whatever, but at the same time like, you want to get attention..." (REC015 SK: L7-9).

Unintentional breaches included situations such as nurses asking and being told about patients not in their care, were due to the "interesting" nature of the patient's case. There were also some indications that "talk" about a patient between nurses had the primary purpose of getting help for their patients. Mention was also made of breaches that were occurring because a nurse was "venting" and needed someone to talk to. It was even suggested that although a nurse may talk in breach, yet it was for the nurse's sanity. Here is how a nurse put it: "...sometimes you have to break almost confidentiality a little bit just for your own sanity it seems..."

(REC021-B-SK: Pg12-L14-15)

Unintentional breaches were occurring during coffee room chats, and lunch room talks. Computers that were left open on carts in the hallways was another weakness. Reminder notes about a patient are a good way to stay on track with respect to patient care. Sometimes, there was the tendency to leave these notes on a counter, med room, or falling out of a nurse's pocket and thus becoming easily accessible to others. There was also apprehension about nurses holding rampant conversations about their patients in the hallway and some were considering reporting this to the authorities. Sometimes patient charts were left laying around, and on other occasions, postings on the Internet, including Facebook and social media for attention. Circumstances like having to immediately return to a previous important assignment could also lead to accidental reveal of otherwise confidential patient information. As one nurse put it,

"...somebody calls you on the phone, you're busy working with another patient, and they call you to provide information about another patient, and automatically your brain just

kicks in and you give the information. But then later on you find out that I can't actually do it ..." (REC022-A-RD-AB: Pg5-L18-21)

5.7.2 Attitudes Towards Breach

A subtheme that featured quite prominently under the breaches theme was "attitudes towards breach". Attitudes could be taken to mean the thought and actions towards breach. Feelings in this area were quite mixed among the nurses that were interviewed. While some expressed displeasure with breaches, reiterating that knowing does not equate to sharing, others suggested that, perhaps, the issue of patient information breach is not taken seriously by the nursing community. Mention was also made that sharing is the second nature of the nurse, with others alluding that sometimes nurses say too much about patients in their care. Some nurses have reported their colleagues for breaches, and have even questioned the adequacy of the consequences for breaches. Other nurses have explicitly encouraged fellow nurses not to breach as they are being monitored – a deterrent. Sometimes nurses had real dilemmas to deal with, as for example, when a nurse witnesses another nurse telling a colleague about a home visit and another looking up files of a patient not in the nurse's care. There was the assurance that information for any famous person was more likely going to be breached.

An interesting comment an interviewee made was that when there is a breach, we do not hear about physicians. This sentiment was expressed when the interviewee candidly said, "...we don't hear about our physician colleagues. So, I think the regulations applying to protection is good, but the regulations involving enforcement is very intense for nurses like, very very protective. Whereas for other healthcare professionals, it doesn't see much follow up ..." (REC019 CA AB: L17-21).

Breaches have occurred because some nurses trivialize patient information protection and have a “not a big deal” attitude towards divulging patient information. This attitude was often imposed by insisting inquirers of patient information. For example, when the interviewees were asked about the attitudes of the inquirer when the nurse could not provide patient information, here is how some responded, “... Oh they’re very frustrated. They’re very frustrated. They want, well they say, “Can’t you just tell me how they are? Can’t you just tell me?” (REC020 CA AB: L10-11). According to some nurses, their biggest concern was the frustration exhibited by these inquirers when they could not give them the patient’s information.

5.7.2.1 Why Breaches Occur. Among the causes of breaches, curiosity (interesting information) had a high frequency of respondents. Unexpected events, humour (finding a patient’s situation funny and retelling the story to others) were also common. Other reasons included entertainment, human nature, pressure from patient’s family, boredom, lack of education, reaction or response, etc.

5.7.2.1.1 Curiosity. Regarding why breaches occur, several responses were garnered from the interview respondents. Important reasons for breaches included curiosity, such as what brought an acquaintance to the hospital or nurses trying to find out if patients they previously cared for were still alive by searching through their record system. A nurse passionately communicated this, and in her own words, “... if you have a patient who has really made an impact in your life as a person and you’ve done a lot for them per se, or they got really sick and you come to work and they’re not there anymore, you kind of wonder like what happened to them a little bit, so I think the biggest breach that I see would be people just trying to see if that person is still alive by searching for them...” (REC004SK:L10-15)

5.7.2.1.2 *Entertaining.* Sometimes nurses found the patient information entertaining. An interviewee gave an account of what had been read elsewhere; “...I was recently reading my professional magazine and I saw actually examples of where people had been disciplined for doing things like posting pictures of patients on Facebook, or body parts of patients, and commenting on things that they thought were quite entertaining, that sort of thing...” (REC009 RD AB:L26-29). Sometimes, nurses found the patient’s information humorous as demonstrated by this statement; “... I really think those are huge breaches, they think it’s funny, or they take it in a humorous way or ...” (REC022 RD AB Pge 7: L8-9)

5.7.2.1.3 *Human Nature.* Breaches have also occurred simply as a result of human nature, the desire to know or get information, and as one nurse explained, “... I think there’s also intentional breaches of people being human, and people being nosy, and they just want to know. And that’s where I struggle, and you know, I understand everybody’s human and everybody makes mistakes...” (REC008 RD AB: L15-17). Another interviewee said, “...breaching is a constant thing that you really can’t stop because we’re humans, we make mistakes...” (REC019 CAL AB: L10-11). The significance of human nature in patient information breach became even more apparent after an interviewee said, “... and then somebody asks you something quickly, you may just say it without even you know, realizing... you’re human so you’re going to sometimes have little slips here and there, but you know generally ...” (REC004 S Pge 5: L29-31).

5.7.2.1.4 *Pressure from Patient’s Family.* Another example of difficult situations the nurses faced was when the family members came in or called to demand information about a patient. When nurses could not provide information without consent from the patient, the

frustrations expressed by these family members constituted significant pressure for nurses. Nurses who were surveyed indicated that family and friends often call to get updates on the patient. Some family members and friends make it look like it is their right to know the patient's information, as indicated by a nurse; "...people's motivations as to why they would want information is different, I think that you know, if it's going to be a family member or a friend that knows the people dearly and are close to them, then they maybe, almost feel like they have the right to know, so..." (REC002SK Pge 8: L21-25). When asked about whether family members called, the answer was swift and emphatic; "...Oh yeah, almost every day too. Yes, people call and, you know, especially nowadays with blended families where sometimes it's not necessarily that person's direct children or their direct connections who are trying to call and get information..." (REC004SK Pge 3: L3-6). One nurse suggested that pressure from family members was their biggest challenge and added that, "Yeah, cause they're always very concerned, or like they need to know every little detail about their family member, so yeah, I've had family members come up to our nursing station and to look, go through their chart..." (REC004SK Pge 5: L1-3). On another occasion during interviewing, a nurse said, "...Well I know we had one patient where the patient had been with us for a long time, and family wanted to look at her chart, and she had given permission for the family to look at the chart, and I thought, I'm just going to double check with our manager..." (REC005SK Pge 5: L7-10). In some instances, family members have been perceived to be invading the nurse's space. One nurse said that, "...family members are more and more commonly coming into the, ... like you know, nursing areas to talk and everything is visible, and papers left around that have patients name and diagnosis on them..." (REC016 SK Pge 9 L6-8).

5.7.2.1.5 Boredom. Boredom was counted as one of the reasons breaches occurred.

Some nurses in down times on shift may surf the Patient Information System like they would the Internet. An interviewee emphasized that snooping occurred as a result of the human desire to get interesting information, and sometimes, just simply to break boredom. A participant put it this way, “... I think if it’s none of your business you don’t have to go looking for information that doesn’t really concern you. And some I think do it out of boredom, curiosity, just to be inquisitive ...” (REC012 CAL AB: Pge 6 L9-12). Another said, “...They want to know, oh something’s interesting, they want to follow up, boredom would be another one...” (REC019 CAL AB Pge 8:L20-21).

5.7.2.1.6 Lack of Education. Breaches that occurred as a result of lack of education was important to nurses. Some of the nurses pointed out that the educational institutions they attended had high expectations for confidentiality. A nurse commented that, “... three months into my program we were in a hospital on a nursing unit and the level of, or the expectation of confidentiality from the education institution was one of the top and upfront pieces of expectations of me as a student, as well as the rest of the students. That, information was accessed appropriately...” (REC008 RD AB Pge 4 L7-10). The same individual remarked that, “...if there were any breaches that the education institution became aware of, there were certainly outcomes that happened...” Concerning lack of education, a nurse reiterated saying, “...I wished there was more. I’m sure the regulations are fine, but I wish there was more education and more discussion with regard to the protection and enforcement. I wish things would be a little more clear cut about what information can be revealed to which parties...”

(REC019 CAL AB Pge 4 L10-11). There was also the belief that breaches continued to occur because there were no explicit gate-keeping to ensure that breaches don't occur.

5.7.2.1.7 Reaction v. Response. Sometimes breaches happened as a result of reaction or in response to a situation. For example, knowing what could have been done and not doing enough to save the patient could get a nurse upset and cause him or her to tell others about the situation. Some nurses pointed out that sometimes if a nurse is in dire need of a solution to a problem pertaining to a patient, the nurse may post the situation online, hoping to get a response from the nursing community. One nurse narrated an incident and in her own words said, "...We had an instance on our ward, this is a few years ago now, where one of the staff, one of the nurses put something on Facebook..." (REC001SK Pge 26 L23-24) Although not a lot of detail was provided by the respondents, there was mention that certain nursing practices were revealing of patient information. For example, having patient names on charts and paper records; "...you need to have their names on the charts. And they are visible for people to see, but all they can see is a patient's name..." (REC005SK Pge 3 L13-14). There were other occasions where nurses had to respond to emergency situations and have had to temporarily leave what they were doing at the time without due consideration to privacy and confidentiality; "... sometimes emergencies happen and you're called to help with an emergency, and if you just leave charts around or information, so that's one thing..." (REC020 CAL AB: L17-19).

5.7.2.1.8 Action v. Inaction. As mentioned earlier, breaches occur due to actions and inaction by nurses. According to the nurses, actions include nurses texting patient information to colleagues in another facility, deliberately and inappropriately accessing information about other nurses, nurses viewing the charts of other nurses on admission, and accessing their own records.

One respondent described leaving workstations on wheels open as the biggest breach. Other actions and inactions included leaving printed electronic materials on desks easily accessible. One nurse described it this way, “... often you know, will see people get up and leave for coffee or leave for lunch and not lock the computer. So then that access, someone else can come and look ...” (REC008 RD AB Pge 5 L8-9). Another commented that, “... biggest breaches I see are the work stations ... the wheels our computers are on being left openso anyone can wander in there... Any sort of printed off documentation. I see lots of people just leaving them in front on desks that are easily accessible...” (REC019 Cal AB Pge 3: L21-24). Conversations between colleagues in public places, emergency calls causing patient information to be left in the open, venting about work at home, and siblings or family relations who are nurses that have the tendency to discuss patients they both know. Breach by taking pictures of sleeping patients and making fun of them or posting these pictures on social media was noted as well. Breach as a result of “elevator talk” was noteworthy; “...Yeah well if, or even just in the elevator hearing people talk yes. I usually don’t say anything because that’s another confrontation to me. But yeah, no it happens a lot and, that’s why I know...” (REC004SK Pge 17: L4-6)

5.8 Theme C - Access to Patient Information

Information privacy and confidentiality hinge a great deal on how readily information can be accessed. Information that is easily available is often considered to be less secure. The opposite is true about secure information. In the following presentation, attention is focused on what the nurses who were surveyed said about access to patient information.

The nurse participants frequently related the topic of access to patient information by the following contrasting issues: accessible (open) v. restricted access; and sharing of information v. protection of information. The generational issue of posting on social media was also mentioned.

5.8.1 Accessible (open) v. Restricted Access

Although the law restricts access to only information pertinent to patient care, in the survey, several nurses indicated having access to a lot of patient information. Statements that pointed to this included the following:

“...we have access to a great deal of information...” (REC008-D-RD-AB: Pg2-L28),

“...everybody’s information. But it’s not necessarily what we do, it’s just so much more available, readily available to us” (REC017-P-CAL-AB: Pg2-L19-20),

“...so if you’re working on 5B surgery and you open your computer database you can get the name of every patient that’s on there” (REC004-SK: Pg3-L21).

The pervasiveness of the electronic record system has added to this access. There is access to levels of electronic information with mention made of central zone electronic medical records and Alberta Netcare System. As mentioned earlier, some nurses said during the interview that sometimes patients provided more information than needed for treatment but also pointed out that access to patient information is variously controlled. There is role-based access control, in principle, with limited access to patient information. Statements that pointed to this or suggested some level of access control included the following; “...if you would have to get a sign in to something, to access that information, then you track who’s looking at what chart...” (REC001 SK Pge 6 L4-6); “...Well, it’s very important. It’s patient privacy and their records need to be kept private. There shouldn’t be access for everyone to see everything. I

wouldn't want my personal health records out there for everyone to see, and I respect patient's health records..." (REC005S Pge 2 L3-6); "... SK Health has a province-wide database, that you're given access to depending on where you're working and what level you need, so the temptation, like as far as I know, they monitor that and routinely do audits..." (REC016 SK Pge 8 L25-28); "... And then my role, I have a certain level of access to the information that I can see and there's pieces of that information ..." (REC008 RD AB Pge 2 L18-19); and, "...I think that's very good. And just because you have access to the system doesn't mean you can access any record which I think is excellent..." (REC009 RD AB Pge 5 L30-31).

The nurses described access to paper records as laborious. At a point, authorized signature was required to view paper records – historical practice. The nurse participants believed that professional regulations are critical to maintaining privacy of patient information (REC008 RD AB Pge 2 L26-27). The participants also believed that professional behaviour meant following regulations. This belief was supported by statements such as "...As I said, as professionals, we have access to a great deal of information and unfortunately (not discernable) there are breaches of that, whether it be intentional or unintentional, and I think you know being cognizant that information is protected....", (REC008 RD AB Pge 2 L27-30); "...I personally have been involved in situations where I actually had to report staff for inappropriate use like where they posted things on Facebook, and that sort of thing, not necessarily that they found it entertaining but that they were just sharing way too much information pertaining to their professional practice on social media sites..." (REC009 RD AB Pge 4 L30 – Pge 5 L3); "...Unless I wish to tell somebody, they don't need to know it, so you can take that personally and professionally. We have to respect people's privacy..." (REC022 RD AB Pge 2 L16-18);

and, "... I think it's a big responsibility for our job as nurses to help to protect the client's privacy, and also it means it's part of our duty, this is what we do because they, the clients or the patients trust us enough to give this information they wouldn't tell anybody else. So I feel like it is our responsibilities to just protect it for the clients benefit..." (REC015 SK Pge 2 L15-19).

There was also the question of where compliance met with professional responsibility. A nurse let her feelings out this way, "...another one would be fear, fear of yourself, like looking up your own patient information that you've received if you're waiting. That is something that definitely does it. Or, fear for a family member. it overrides your professional obligation cause you want to do it..." (REC019 CAL AB Pge 8 L24-27). Another nurse expressed frustration with caring for the patients. And so sometimes you might need to ask somebody for certain information. Like when I used to work in the hospital for instance, a patient might come to the hospital, the only person that they will, there are patients that really don't have family members. Or sometimes they have friends and they come to the hospital, and they have not indicated who to give information to..." (REC022 RD AB Pge 4 L26-31).

5.8.2 Sharing of Information v. Protection of Information

In the nurse's role as a liberator of information, sharing is important. The more information available for the patient, the better the care. Nurses have avenues for sharing that include other institutions, and working with other professionals such as social workers. Often, different health professionals need different aspects of the patient's information from the nurse. Another avenue is free, unrestrained sharing using verbal, email, and others as pointed out by this respondent's statement; "... we've had instances where people have shared information through mediums like email, through faxes, through copying, scanning..." (REC012 RD AB

Pge4 L3-4). Nurses shared not only patient information but system login information such as “password” as well, sometimes with a number of nurses operating under one login credential. There were instances of lack of understanding of legislative pieces that have prevented useful information sharing. One of the nurse’s dilemmas was knowing what information to share with the patient and yet, having to wait for the doctor to do the sharing.

Other issues nurses had to deal with as part of their daily activities were talking about patients who were back to the hospital a few more times, family members requesting to see a patient’s chart, and patients requesting that certain individuals cannot be told information about him or her. Regarding what information was shared and how they were shared, the respondents mentioned several types of information using different avenues: *Facebook sharing and sharing with family members*. Other statements that pertained to sharing by the nurses that were interviewed included the following; “...when a family member or anybody calls in to ask information about a patient’s condition, we always check on the care plan that we have, as to who is allowed to receive information over the telephone, and that would be documented, or the next of kin, we give information to. Or if there’s an advance care directive and it states clearly, we know who is allowed to receive information...” (REC004 SK Pge 2 L23-27); “...cause I’m a fairly new nurse, so when I experience things for the first time, I may want to sometimes share that with other people...” (REC004S Pge 8 L19-20); “...but there is definitely times when they ask questions and I for sure give probably more information than I should...” (REC021 SK Pge5 L26-28). “... But right now, it doesn’t really matter, like if family calls we’ll say yes they’re in the hospital, and some nurses will leak information out, without that person’s approval...” (REC013 Sas L10-12). Other than family members of the patient, sometimes outside agencies

such as the police call to inquire, expecting that nurses would freely share patient information, as indicated in the following statement; “...sometimes we get like police officers calling. And that’s a hard one because lots of times we will say like sorry we can’t give you that information about this patient, and they’ll keep kind of pushing for it...” (REC021 SK Pge8 L18-20). Some nurses generally appreciated the privilege of been chosen as confidants and called for all nurses to be intentional about protecting patient information. One nurse passionately expressed the feeling this way, “...I mean lots of clients tell me stories that they wouldn’t share with some other people, even if they’re families and close friends. And things they would just sometimes share with someone. I think, sometimes I feel honored they chose me to be the one to share with me, and I feel obligated to just help them to protect this. Not share with anybody including family and their close ones...” (REC015 SK Pge2 L23-28). A nurse who was very concerned about sharing of patient information voiced another disturbing concern, sharing of logon credentials such as usernames and passwords among peers. In the nurse’s own words, “... we continually struggle with clinicians understanding what their role is in maintaining that privacy level.

Elements of the demonstration of that difficulty could be scenarios such as staff sharing passwords and usernames, when it comes to information systems. They’re not aware that if a person basically shares a password or username, we lose the capability of auditing to see who actually was in the system...” (REC012 RD AB Pge 3 L25-29). In some instances, nurses have been proactive when it came to protecting patient information. The following is what a nurse said she did; “...if family members are present when we’re giving report off to the next nurse, I’ll often ask them to step out, especially if it’s not about their family member, or their person

they're visiting, it's just not, for the protection of the other people in the room..." (REC016 SK Pge 3 L10-13).

There was the suggestion by some nurses that electronic records have improved the protection of patient information. This suggestion was expressed in the statement that follows; "...I think that having electronic database for accessing patient records electronically is going to be able to protect patients confidentiality and privacy much easier because if you have a paper chart and that's on a desk, it's a lot easier to open that up and..." (REC02S Sask Pge6 L7-10).

There were also those who thought that paper records provided more confidentiality. One said;

"...I think in terms of confidentiality, I think the paper definitely is a better way to protect someone's, you know, like who they are, what they're there for. Whereas computer access, so much of it depends on who has a password to access ..." (REC004 Pge9 L8-11). In order to safeguard patient information, the nurses said that education and clearly understanding the consequences for breach were important; "... I think the key thing is education. Just teaching people how important it is, and explain to them you know if you get caught there's penalties.

And, I think that needs to be emphasized. Education is always very important with anything. You know that's how you learn things and that's how you can change too is through education..." (REC005S Sask Pge11 L3-7). Another reiterated during a separate interview that, "..., I think, you rarely see, or I've rarely seen any kind of outcome for breaching information, and I know there's checks and balances in place, but I wonder if there should be more audit trails ..."

(REC008 RD AB: Pge 3 L7-9). Nurses do not only think it is their responsibility to protect patient information but also feel it is their obligation as well, as one nurse put it, "...I think it's a big responsibility for our job as nurses to help to protect the client's privacy.... I feel obligated to

just help them to protect this. Not share with anybody including family and their close ones...”

(REC015 Pge2 L15-16, 26-27).

5.8.2.1 Social Media. A specific form of sharing that has attracted considerable attention involves the use of the social media platform. There was no denying by the interviewees that nurses have, on a number of occasions shared patient information on social media. The statement that follows exemplifies this; “... We had an instance on our ward, this is a few years ago now, where one of the staff, one of the nurses put something on Facebook. The nurse didn’t identify any names, but it was enough information that other people who were working at that time, could identify based on the information that the nurse provided...” (REC001 SK Pge6 L23-26). Social media posting is seen as a generational issue. There was the belief that younger nurses posted to social media to get help from more experienced nurses. A young nurse shared her thoughts and experience on this matter this way, “...Because our generation, the social media just is like, not posting information about your patients. Because I’m a fairly new nurse, so when I experience things for the first time, I may want to sometimes share that with other people...” (REC004 SK Pge8 L17-20). Some believed that posting information about the patient without explicit disclosure is safe. Sharing patient information online is perceived as an avenue for venting, and as a nurse put it, “... I think you’re right, I think a lot of it is venting and they just want someone to talk to or, they post everything about every other aspect of their life, so why not about work? ...” (REC021 SK Pge11 L21-23). On other occasions, venting occurs as nurses share their experiences with family; “...Yeah, if I discuss my shift at work, I don’t use names, I don’t you know, when you just go home and you talk about your day, you know you vent...” (REC005 SK Pge4 L11-12). Some interview participants indicated that sometimes if a nurse

found a patient's condition he or she considered humorous, it could be posted on social media for the sake of sharing a joke. A participant put it this way; "... I was recently reading my professional magazine and I saw actually examples of it where people had been disciplined, for doing things like posting pictures of patients on Facebook, or body parts of patients, and commenting on things that they thought were quite entertaining ..." (REC009 RD AB Pge4 L26-29). There are also those nurses who see nursing as their lifelong adventure and would like to report and share events that occur on this journey. According to one interviewee, "...I think they're probably just trying to tell, you know like on Facebook people just like to tell crazy stories about things that have been happening to them, so they think it's part of their life too ..." (REC006S Sask Pge7 L6-8).

5.9 Theme D - Education of Patient Information

Education in patient information, particularly in privacy and confidentiality is critical to protecting patient information and maintaining its integrity as well. Education would alert nurses regarding proactive steps to minimize patient information privacy and security breaches, and provide the knowledge and skills needed to deal with privacy and confidentiality issues. The broad theme of "Education of Patient Information" is an umbrella for several other sub-themes including awareness versus ignorance, adequate knowledge versus lack of knowledge, and specific education versus insufficient education. The next few paragraphs present the results pertaining to the theme and sub-themes mentioned above.

5.9.1 Awareness v. Ignorance

Education by Alberta Health Services (AHS) is designed to raise patient information privacy (PIP) awareness. Nurses learned PIP in nursing school and through mandated training

modules. Privacy concerns were part of ongoing professional development for nurses. They saw learning PIP as an obligation and used breaches as moments for education. When the question was asked of when and how knowledge in patient information privacy was acquired, the interviewee responded, “... That started right from day one of my undergraduate nursing where it was, you know three months into my program we were in a hospital on a nursing unit and the level of, or the expectation of confidentiality from the education institution was one of the top and upfront pieces of, or expectations of me as a student body as well as the rest of the students that, information was accessed appropriately, was respected, was kept confidential ...” (REC008 RD AB Pge4 L6-11). Another nurse called attention to the need for nurses to be aware of some technical measures in place to protect patient information, including measures that audit patient information access; “...you need to be aware people monitor confidential or high profile charts, and not to look, that they will find you, and they will dismiss you...” (REC017 CAL AB Pge8 L14-16). It appeared that the nurses were appreciative of the work Alberta Health Services is doing in the area of patient information privacy awareness. A statement from a respondent that summed it up said, “... so AHS has, you know they do great work every year to ensure that we have education in this area, and all nurses are very very much aware, all very aware of keeping the patient’s information private and confidential...” (REC022 RD AB Pge2 L23-26).

Some of the nurses surveyed had difficulty connecting theory with reality. Others said they did not learn enough about privacy in school. There were those who suggested to teach PIP to improve best practices and called for a forum or platform for practicing nurses to actively discuss patient concerns privately. According to a relatively high frequency of interviewees, nursing school and annual training through AHS provide privacy education with the expectation

to observe patient confidentiality occurring early in nursing education. Most nurses said they received privacy knowledge and awareness through school, orientations, professional development, mandated training modules, fellow nurses, and in some cases through reminders. However, some expressed the need for more explicit education in regulatory compliance, and understanding of security platforms.

There were others who suggested that breach incidents should be used as open education moments for nurses. The nurses also said that privacy education should carry the same message for all nursing units, targeted or tailored to inform new nurses and update existing nurses. Respondents believed that education in privacy could help curtail breaches. The need for a platform for practising nurses to discuss privacy concerns was raised. Lack of such platform makes nurses destress by speaking publicly; "...I think one of the big challenges is not having a forum to be able to really discuss patients concerns, to actually be able to debrief with someone confidentiality, confidentially and privately. That leads people to want to speak in public to destress and deflate situations..." (REC019 CAL AB Pge5 L23-26)

5.10 Theme E -Nursing Practice

As mentioned earlier, nurses provide the largest portion of direct patient care. Nurses focus on medical treatment, following prescribed instructions, and maintaining routines; providing information, giving service, and coordinating care and treatment; seeing patients as vulnerable people, helping and supporting them as individuals; and, inviting patients to participate in the caring process and encouraging them to take responsibility in their own care (Jangland & Larsson, 2011). While discharging their duties best as they could, nurses are faced with some challenges. These include carrying out their professional obligations while dealing

with the human nature that often goes against professionalism, how to cope with challenges and their consequences, use of privacy infrastructure, pressure from the patient's family, safe versus unsafe practices, trust versus mistrust.

5.10.1 Professional Obligations v. Human Nature

Professional obligations of the nurse include accessing a plethora of pertinent information in order to make good judgements about a patient's situation. A number of the respondents said or implied that, "...as professionals, we have access to a great deal of information..." (REC008 RD AB Pge2 L27-28). A respondent also mentioned that, "... I think the AB Health Service, the provincial, the federal and professional regulations are critical to maintain privacy of information (REC008 RD AB Pge2 L26-27), and further added that "...I know there's a level that if you're a professional that's a professional responsibility that you only access what you should..." (REC008 RD AB Pge3 L11-13). Also, the professional bodies to which the nurses belong have responsibilities to the public and the law; "...the professional body, when it receives those complaints, they have a responsibility to the public and to the law to investigate that..." (REC008 RD AB Pge7 L4-6), and called on nurses to be respectful of patient information. Concerning professional obligation, this is what a nurse had to say; "...but now that AHS is a very large corporation, they have, there is a number of forms we sign and there's also modules that are mandated for us to complete. And so for those reasons I feel secure in my knowledge of how not to breach. and also, I think there is an ethical duty to conform..." (REC017 CAL AB Pge5 L26-29). The word "professional", was also often associated with "trust" by the respondents, as indicated in the following statement; "...to me, patient information privacy is basically the forefront of all our information protection practices. It is basically the protection of

patients' data, vital information to allow for trust to be built between the healthcare professional as well as the patient itself..." (REC019 CAL AB Pge2 L7-10)

The human nature of the nurse is defined in terms of their role, beliefs, actions, likes and dislikes, character, feelings, and personality as they relate to patient information. The nurse was described as being dichotomously a protector and liberator of information, and a believer in the flexibility of information availability. According to the nurses, sometimes the natural tendencies such as a strong desire to seek information can be overpowering to the point that it could subdue the nurse's professional obligation, as demonstrated by the statement from an interviewee; "...Well human interest, and human nature..., a desire to get information, a desire, human interest. it's a bit of snooping. They want to know if something is interesting, then they want to follow up If you know it's a famous star that you really love and they're on your unit but you're not in care, you would like to find out why he or she is here. Another one would be looking up your own patient information Or, or fear for a family member. It overrides your professional obligation ..." (REC019 CAL AB Pge8 L15-23).

The nurse can also exercise restraint and is disciplined. At times, the obligation nurses felt to protect patient information came not only from the duty to comply but as a result of the privilege of being chosen to be the recipient of someone's very personal and confidential information. A nurse expressed this appreciation in her own words when she said, "...I think sometimes I feel honored they chose me, to be the one that's to share with me, and I feel like this other information, I feel obligated to just help them to protect this. Not share with anybody including family and their close ones. Because sometimes like I said, this is really private information, they are willing to share with me..." (REC015 SK Pge2 L25-29). Other defining

characteristics used by the nurse included putting herself or himself in place of the patient, and being on the other side. The nurse is not afraid to befriend the patient, and at the same time able to share information. He or she would protect the integrity of patient information by all means.

Acknowledging the importance of the commitment to protect patient information, a nurse said, “...I think it’s a big responsibility for our job as nurses to help to protect the client’s privacy, and also it means it’s part of our duty, this is what we do because the clients or the patients they trust us enough to give this information they wouldn’t tell anybody else. So I feel like it is our responsibilities to just protect it for the clients benefit...” (REC015 SK Pge2 L15-19)

A respondent described the nurse as an individual who would exercise restraint against “human nature” in order to stay disciplined about privacy. A nurse put the issue of human nature and its tendencies this way, “... you’re human so you’re going to sometimes have little slips here and there but you know generally, the more you work and the more experience you have, the better you are at just kind of building it into your natural...” (REC004 SK Pge5 L30 of page 5 to L2 of page 2). The same respondent commented later that, “it’s human nature to be nosy”.

Another respondent said, “... you know, its human nature, you want to talk about these things. And that’s ok, as long as it’s kept in that confidential manner...” (REC005 SK Pge6 L25-26).

Regarding the question of human nature, a nurse humbly said this, “... One of our weaknesses, people like to look into things that we are not supposed to, but at the same time you have the curiosity about, oh you always ask, or check and see, but then things like this, that’s why I think they have to have the boundaries...” (REC015 SK Pge11 L8-11). There was yet another notable comment relating to human nature that said, “...I think it’s just human curiosity and, maybe just how much the world has become so electronic that it doesn’t seem wrong because we’re just, it’s

just so available all the time. But I think we'll have to really maybe not necessarily snoop..."

(REC016 SK Pge8 L13-16).

The idea of breaches occurring as a result of human nature reverberated through many responses. Some indicated the nurse's dislike for bureaucracy and the tendency to not follow the rules, with some justifying why a rule was broken. For example; "... I've broken the rules. And I've taken a picture with my cellphone, and I've shown them, and then I show them ok. You watch me, I'm deleting this, and I'll delete it in front of them so that they know that it's not in my phone anymore. So if I break the rules a bit, I always make sure that the patient, is aware that I'm not supposed to do this, but I'm going to do it just for you..." (REC005 SK Pge7 L15-20).

On the subject of the use of rules and regulations in nursing practice, here is a comment from a respondent; "...I think you know sometimes it's hard because, we have, we understand what patient privacy and confidentiality is, but at the same time there's also a push for family centered care. And bedside rounds and things like that, so sometimes it's kind of a fine line between family-centered care and patient privacy..." (REC021 SK Pge3 L17-21). Nurses had the feeling of friendship when a patient shared. Participants mentioned that a nurse would put himself or herself in place of the patient as they have been patients before. In terms of patient information exchanges, the nurse was described as having a "dual individual perspective" since the nurse used to give information but is now receiving information. In the respondent's own words, "... I can just have two-sided experience now. I used to be the one giving away the information, but now I sometimes have the frustrations about trying to get information..."

(REC015 SK Pge4 L29-31).

5.10.2 Challenges v. Consequences

There were many challenges faced by nurses in patient information privacy. Challenges are setbacks that negatively impact the proper adherence to patient information privacy practices.

These setbacks, according to the interviewees, could be as a result of the nursing practice environment, pressure from patient's family, and peculiar situations.

In nurses' conversations about patients, there could be pressure from colleagues to divulge full patient identity. Nurse participants indicated that nurses who were not in charge of a patient could come in to read a patient's chart, adding that sometimes nurses got frustrated because while they were working hard to maintain privacy, other nurses enabled leak outs. Some nurses suggested that "peers not following the privacy practice can wear out those who do".

The user unfriendliness of the patient information system interface was sometimes a challenge as well. Nurses had the notion that parts of patient information regulations were restricting. A nurse commented, "...I can't even ask their daughter a question without their consent, if they're not able to give me that consent at this moment, I'm kind of, stuck..." (REC022-L-RD-AB: Pg3-L17-21). Sometimes nurses are "caught between a rock and a hard place", as a participant recounted, "...Yeah, it's hard as a nurse because our main goal and focus is caring for the patients. And so sometimes you need, you might need to ask somebody for certain information.... When I used to work in the hospital for instance, a patient might come to the hospital, the only person that they will know there are patients that really don't have family members. Or sometimes they have friends and they come to the hospital, and they have not indicated who to give information to, and they are at a point where they're not able to give that, authorize somebody to be able to access their information. And here is this friend, or this neighbor, that brought them to the hospital, and now they are wanting to receive feedback about

the patient. If there's nothing written down to say that they can have that information, they can't have it. So that's a dilemma..." (REC022 RD AB Pge4 L26 – Pge5 L1-5).

5.10.2.1 Privacy Infrastructure. Another challenge that nurses faced was the locations of their nursing stations which in some cases were in public view. A participant expressed concern in this area this way, "...breaches I see are the work stations, the wheels. Our computer on wheels and being left open so anyone can wander in there. Any sort of printed off documentation. I see lots of people just leaving them in front on desks that are easily accessible..." (REC019 CAL AB Pge3 L21-24). In a separate interview, another participant indicated similar concerns by making the statement; "... one of the challenges is in regards to the layout of my workplace... our nursing stations are in the middle of the hallway. And the charts are right up against the hallway, so I mean you can read the person's name right there..." (REC001 SK Pge5 L1-3). Although not designed with security and privacy as the primary goals, several participants mentioned electronic records when the question of security and privacy of patient information privacy came up. A participant's response said, "...there would literally often be volumes of paper documents. So you didn't always have the full picture because you could have twenty pounds of paper documents locked up down in health records, and if you wanted to see that, you would have to request it, and it could take two or three days for that, those charts to arrive for you to access. Whereas the electronic world, that person, as long as they've been connected to that system, everything is viewable. So, in terms of obtaining information, it's quicker, I mean once you know where to go and look for it. If I was working in critical care, that could be very important, delivering timely care that's needed, because everything is at your fingertips, whether it be lab results, whether it be diagnostic imaging results, it's there and within

a snapshot of a second to see. ..." (REC008 RD AB Pge5L25 – Pge6 L3). Nurses were also aware that some of the systems (technology) they use for their day-to-day activities have built-in security and privacy features. A participant said, "...nowadays most of it is electronic. So things like, there are default checks once you even leave your work station, in two or three minutes... it shuts down. So the next person cannot read what you were working on, they cannot do anything on your work-station. So all these privacy checks that help us to make sure we keep..." (REC012

CAL AB Pge2 L29 – Pge3 L2).

The privacy infrastructure includes avenues for reflection. A respondent said, "...Yeah reflection is a huge part of the job. I think there's situations where colleagues are talking about other, talking about patients, or talking about rather intimate details about the person. And they're in rather public areas. And I think about what is the most appropriate way of dealing with the situation..." (REC019 CAL AB Pge4 L30 – Pge5 L3).

5.10.2.2 Pressure from the Patient's Family. Nurses had to deal with pressure from the patient's family to provide them the patient's information, and having to deal with angry family members. There was the suggestion that family is the biggest challenge to dealing with patient information privacy. This was gathered from the response to the interviewer's request for the interviewee to tell him about a situation or situations where interviewee was confronted with patient information privacy issues, or dilemmas, and how the interviewee's success or failure in dealing with them made the interviewee feel. The answer was a rather terse but intense "I think family is our biggest challenge" (REC004 SK: Pg4-L28).

In some instances, family members expressed frustrations, expecting the nurse to have every information imaginable about the patient. Peculiar challenges that were pointed out

included modalities for redirecting inquiries to designated family members, when friends call to ask about a family member that has died, the issue of personally liking a patient, the News and Police demanding to interview a special patient, and marrying privacy and confidentiality with family care. There was also the difficulty of asking family members to step out during rounds, the dilemma of when the patients cannot speak for themselves and the nurse is not sure what to do. This is what a nurse said she would do; “.....the patient may be unresponsive and can’t talk. So, in those instances you really have to use your ... so sometimes to deal with that one, I would go to the family member at the bedside and say, listen this person’s on the phone, can you please come and take the call...” (REC004 SK Pge6 L29-30 to Pge7 L1-2). In another instance, a participant expressed similar sentiment by saying, “... if a patient can’t really speak for himself... themselves, or they might not be stable enough to give that permission for their family members, and so then it’s kind of like a battle with yourself and the family member...” (REC004S SK Pge5 L8-10). Another nurse said, “...on a daily basis it would mostly be like I said, a lot of our patients are sedated and can’t speak for themselves, so it would be speaking with their family, and sometimes their friends kind of about what’s going on without revealing certain things about the patient. We work with the social workers a lot to figure out who the next of kin is, we can give information to, to help make decisions, and then sometimes it’s difficult when other family members want to know information and you, just can’t give it out...” (REC021 SK Pge2 L27-31 to Pge3 L1-2).

5.10.2.3 Consequences. Not knowing or ignorance of the consequences for breaches was mentioned as a reason for breaches. Some of the consequences of breaching that were mentioned included a nurse losing a license, legal action, and suspension. A nurse stated that, “...we

appreciate the idea that information released can violate that trust. In many ways I think many view that as more of a fear of legal action or losing one's licence..." (REC019 CAL AB Pge6 L9-11). This awareness was confirmed with utterances such as, "... there's a boundary knowing that it's somebody cares about this information besides us, and that there can be punitive damages should you break that trust..." (REC017 CAL AB Pge2 L27-29). Breaches may go unnoticed for a long time, and sometimes nurses have felt the power of letting a patient present how a breach has affected him or her. Nurses in general have often taken the heat when there is a breach. In some cases, the consequence of breach has been termination. A participant recounted an incident that occurred; "... People were accessing a patient's information inappropriately, where there was a follow up and to my knowledge either nurses lost their licence or were terminated for accessing this patient's information improperly..." (REC019 CAL AB Pge7 L27-29).

A participant commented that nurses tend to be blamed whenever there was a breach, and expressed her sentiments this way; "...regretfully whether this is just a bias because of my position, or bias based upon media, which most likely it is, it seems that nurses in general, take the heat if there is a breach of information..." (REC019 CAL AB Pge4 L13-15).

5.10.2.4 Safe v. Unsafe Practices. Privacy also meant 'safety' of information from outside parties. A participant insinuated that it was almost impossible to guarantee the safety and thus, privacy of patient information. This participant put it this way, "...Cause not everything is private. Like in a perfect world, everyone would have a private room but that doesn't happen. So, I think sometimes what like the professional bodies are asking for confidentiality it's just not realistic with what we have available to us..." (REC021 SK Pge3 L24-27).

In order to safeguard patient information, nurses on duty are often alert to what is happening in the patient's environment. A nurse narrated part of a common nursing practice she engages in; "...I guess what I do every day is you know I kind of watch like who is coming in and out of the room, I try and communicate with the patient, who they want there, who they don't want there, who they want information given to and that also kind of watching like who's looking at the chart. If it's you know hope, like not hopefully a curiosity thing. If someone's not directly involved in their care you kind of question like you know, who are you? What service are you in?" (REC021 SK Pge4 L13-17).

Other patient information safety practices included nurses using their discretion to deal with particular situations such as this response to a phone call requesting patient information; "...when we get phone calls from family members, there's really no way to verify who they are, so we kind of, have to take it ... if they say well I'm their daughter, we kind of have to take it like, ..., I would check, I try and give information in a general way out, so for example if they phone, they're asking if they're ok, and I'll say yeah like they had a good night, they're stable and then I would kind of encourage them to come in..." (REC021 SK Pge5 L20-25).

Information safety precautions include routine audits to monitor access to patient information and as one nurse put it, "...I don't know how secure it is, I.T. safety things are, and I mean I don't know how often they do the audit and really look into and see, how often are you looking into the information that you are not supposed to, and so..." (REC015 SK Pge9 L2-4).

Regarding safety of patient information, some nurses believed that paper records tend to provide natural protection to ready access, as stated by a participant, "...paper records is to keep the chart physically safe..." (REC014 SK Pge8 L1). Other nurses think that electronic records

make it easy to keep information safe, saying things like, “...I think that having electronic database for accessing patient records electronically is going to be able to protect patients confidentiality and privacy much easier because if you have a paper chart and that’s on a desk, it’s a lot easier to open that up and look or walk by and take a quick look at, you ..., private medical document...” (REC002S SK Pge6 L7-11). Other participants echoed this thinking in their own words including one that said, “...in some ways patient information might be safer with online records, if you would have to get a sign-in to something to access that information, then you track who’s looking at what chart...” (REC001 SK Pge6 L2-5). Here is what another participant said pertaining to safety of patient information; “...Hire a very good network administrator. That is a key part to keep it protected and safe, and I think having, ..., when you’re hiring new staff through, you know, all the education programs. I think the key thing is education...” (REC005S SK Pge11 L1-3). A homecare nurse participant explained a dual-recording practice that helped keep patient information safe and said, “...providing that avenue to ensure that the patient’s information is actually safe, what do I mean by this. For instance, we use charts, ok? We use paper charts and we also electronic information. So, we chart in the computer and we also chart on paper. So sometimes those charts we drive around with them as homecare nurses. So there is a possibility of, for instance when you go to a client’s home, of leaving the chart there...” (REC022 RD AB Pge2 L15-22).

In terms of safeguarding patient information, a nurse indicated that it was a discipline that was drilled into them as students and also as nurses when she stated, “...a lot of it is drilled into us in school, but also our annual education and required education...” (REC022 RD AB Pge3 L28-29).

5.10.2.5 Trust v. Mistrust. The trust relationship between nurses and their patients in terms of privacy was evident in the data. The nurses acknowledged that patients trusted nurses with their personal information, regardless of what form it was in. According to a nurse, “...patients have a right to privacy and the provision of healthcare services, and the people providing that need to take the confidentiality seriously whether or not it’s in verbal communication or written communication, or else it could be electronic communications, and that’s part of the job that’s expected and that patients have a right to...” (REC009-M-RD-AB: Pg2 L12-14).

As mentioned earlier, there was the supposition that nurses are in a position of assumed trust, and that patients share freely with nurses as a result of trust. A participant expressed it this way, “...I think it’s a big responsibility for our job as nurses to help to protect the client’s privacy, and also it means it’s part of our duty, this is what we do because ... the clients or the patients trust us enough to give this information they wouldn’t tell anybody else. So I feel like it is our responsibilities to just protect it for the clients benefit...” (REC015 SK Pge2 L15-19”). Another said, “...I think it is because health conditions are a personal thing for everybody, and they come to the hospital to, and they trust us to keep their information confidential...” (REC006 SK Pge2 L12-14). Still on the topic of nurses and trust, a respondent indicated that trust comes with responsibility, as noted here; “...patients are able to trust the health system, and trust the employees that work in the health system that their information is kept confidential. It also means that their patient’s information is kept in a secure online system if there’s going to be online records or computer records that is kept safe and not in a way that outside parties can access that information...” (REC001 SK Pge2 L15-19).

In some situations, there were no verifications in accessing patient information. Access was based purely on trust. The nurses believed that patient information privacy led to information protection practices and built trust between patient and nurse. Some even went as far as alluding that privacy was an established trust between the nurse and patient.

The thought of the possibility of punishment for breaking trust was also entertained by nurses. There was the awareness of audits for monitoring purposes, and the honour the nurse felt when patients shared, and to quote this nurse, "...I sometimes feel honored they chose me, to be the one that's to share with me, and I feel like this other information I feel obligated to just help them to protect this. Not share with anybody including family and their close ones..." (REC015

SK Pge2 L25-28).

5.11 Theme F - Electronic Records and/or Paper Records

As mentioned earlier in the literature review, the EHRs capture patient information in digital format and make the information available to other healthcare stakeholders (Angst & Agarwal, 2009). EHRs allow for interoperability of health information. The EHRs represent the ability to easily share medical information among stakeholders and to have a patient's information follow him or her through the various modalities of care engaged by that individual.

Paper records are hardcopies of a patient's medical information often physically present in a filing system. Each record method has its advantages and disadvantages, and the nurses who were interviewed had several comments regarding their security, vulnerabilities, etc. Nurses have a dilemma when it comes to the use of electronic versus paper record and security of such records.

5.11.1 Secure v. Vulnerable

Data collected during the study indicated that many of the nurse participants think electronic records are more secure than paper records. The reasons they provided included the suggestion that paper records can be easily accessed by anybody, perception that electronic records have more safeguards such as pop-up warnings, electronic records are a little more difficult to access as good knowledge of the system is needed, and electronic records can be tracked or audited. The following are some of the comments and statements that support the assertion that electronic records are more secure; “...I know now with electronic access everything is monitored and date and time stamped, but it doesn’t necessarily identify why they’re accessing the information...” (REC008 RD AB Pge3 L9-11), “...I do feel that electronic record keeping is better because there are more safeguards. I think I shared with you before how I know I have never had this, but other colleagues have told me that they’ve had things pop up that said, “Should you be accessing this record?...”(REC009 RD AB L25-28), “...with the electronic if people are diligent with signing out, even if they don’t sign out, it is, you have to have really good knowledge of the system to look up your family member, and to access that...” (REC020 CAL AB Pge7 L28-30).

Respondents who believed that paper records were more secure argued that trespassers could be easily seen fiddling with paper. Paper records cannot be accessed remotely; “...So I’ll just start off with like paper records, paper records are, don’t, unless they have been entered into a computer system, are physically there. Nobody can access from a remote site to get a hold of the patie... of a file. That’s a, a protective factor...” (REC019 CAL AB L24-27), adding a level of security to paper records. A participant who thought paper records are more secure than

electronic records said, “...I think paper is harder to access, so it is probably more secure, electronics can be hacked...” (REC005S SK Pge9 L17-18).

Some paper record vulnerabilities were highlighted. Among the vulnerabilities were stickers on paper files that revealed a patient’s identity. They indicated that misfiling of paper records could lead to inaccurate patient information possibly leading to misdiagnosis. Easy misplacement of paper records was another vulnerability. In the past, paper records were taken home and lost, and in some cases, the loss could be permanent. A nurse described an incident where a patient seized paper records from a nurse. These were her words, “...so she actually printed part of the chart and showed the patient, and the patient actually stole the paper out of the nurse’s hand and wouldn’t give it back” (REC020-M-CAL-AB: Pg8-L24-25). One of the few who saw no difference between paper and electronic records commented, “...Hacking or like just leaving your computer open to anyone to see, but it’s the same thing with papers though, anyone can access paper information. So there’s really, I don’t think that there’s any difference...”

(REC004 SK Pge10 L4-6).

The use of paper records appeared to be pervasive in the Saskatchewan Health Region. The following are examples of comments and statements from the nurses in the Saskatchewan Health Region in support of the paper records pervasiveness: “...right now we use paper records in our Health Region, or mostly. Some units, emergency has transitioned to electronic, but where I work we still use paper records...” (REC021 SK Pge8 L25-27); “...we’re still quite paper based, though we are slowly getting closer to electronic based...” (REC016 SK Pge8 L8-9); “...so far, paper is what we are doing, I think it’s ok the way it is now...” (REC015 Sask Pge9 L23-24); “...The patient information that, in Saskatoon for the, medical and surgical ward, most

of them are paper based. It's not like electronic based..." (REC014 SK Pge3 L6-7); "...Well, where I work, our charting is all, it's still done on paper. We don't have, we don't use the computer for our charting. We did at one point, I'm at City Hospital and we went to computer charting for a while and now we've gone back to the actual chart..." (REC005 SK Pge2 L22-25), "...Well as I say, we don't have a lot of electronic records. but you know, I will say, I was just in Foothills in Calgary in May for four days, my cousin had major surgery and I was with her for four days in the hospital. And they do all of their charting at the computer..." (REC005 SK Pge9 L25-28); "...I know the other two hospitals, well R.U.H. like the University Hospital, they're I think they're fully on board now with the electronic health records. But Saint Paul's, we're just getting introduced to it, so we're still doing paper stuff right now..." (REC004 SK Pge9 L1-3); "...Well, on the floors in our hospital it's all paper, and emergency has just gone to electronic charting. So, there's currently both right now so, I think we're gradually getting to all..." (REC004 SK Pge8 L26-28); "...right now, I deal more with paper records but there is a movement toward electronic charting and our health region is a little bit behind in times compared to maybe Alberta or America..." (REC002 SK Pge6 L23-25); "...Ok, my experience is mostly on paper copies like we're still doing the paper charting on our ward..." (REC001 SK Pge2 L23-24); "...The only things that are on the computer right now are the bed placement that has which bed each patient is in and so if you're going to admit or discharge a patient or transfer room to room, that is done on the computer, but all my charting and medication records, everything like that is on paper..." (REC001 SK Pge5 L22-25).

Skepticism regarding the use of technology was sometimes used to justify the continued use of paper records. For example, one respondent while not explicitly commending the use of

paper records made this comment, “...So, in terms of which is, I think you know it’s like anything with technology, when it works and it’s the right software for what you need, then it’s great, but if you get so reliant on it that when it goes down, systems don’t function anymore then there’s problems. So I can see why paper is still kind of used so much. Unfortunately, we waste so much paper at work, it’s unbelievable...” (REC004 SK Pge9 L3-8).

In AB, it was not uncommon to hear statements such as, “...So we access everything, almost solely electronically...” (REC008 RD AB Pge4 L24) and stories about adverse previous experiences with paper records were used to illustrate their preference for electronic records.

Here is an experience from the participant’s own words:

“...Now with paper charting, problem is you don’t know who took the chart, once we were, I was taking one of my patients to have a procedure. We looked everywhere for his chart. This other time we were using charts in the hospital. We couldn’t find it and you can’t send a patient to the O.R. without a chart. We looked and looked and looked and I decided to just walk into the doctor’s lounge, because I’m like where else, you know?

And lo and behold it was in the doctor’s lounge. One of the residents had taken it there...” (REC012 CAL AB Pge4 L8-14).

Although they may be using a hybrid record system, when participants in Alberta talked about paper records, they would often make it seem “a thing of the past”. For example, a participant would say, “...I learn every day, I learn something new every day, it is a massive change management field to introduce a clinical information system into the healthcare setting. It opens up things like privacy, what people don’t recognize or realize is that in the past with paper based processes ...” (REC012 RD AB Pge4 L31 to Pge5 L1-3). Another nurse said this in

reference to paper records and the past, “I think because I’ve been nursing for thirty-two years, it’s grown and it has blossomed into a different feeling, at the beginning of my career it was all paper...” (REC017 CAL AB Pge2 L11-13). The same participant later added that, “... I think paper is too onerous...” (REC017 CAL AB Pge5 L3).

While participants pointed out the shortfalls of the paper records system, they were quick to load the electronic record system with accolades. A respondent said this, “..., whereas when you had papers, you would only bring as much as you could carry, so it’s just I think it’s efficient to have electronic for ease of portability, and I think it’s wonderful having electronic information at my fingertips ...” (REC017 CAL AB Pge6 L1-4). A participant remarked that, “...Calgary switched over to, the program called S.C.M: Sunrise Clinical Manager a few years ago...” (REC020 CAL AB Pge6 L30-31) possibly around 2012.

5.11.2 Benefits v. Pitfalls of Electronic Records

In terms of the benefits of electronic records, there was the belief that electronic records cut down on paper floating around, electronic records could self-protect using techniques such as screen shut down when left idle for a certain period of time. Statements from the participants that favoured electronic records included, “...I think for electronic records, it’s for me a better option because you can trace whoever is looking at things that they are not supposed to be looking, there’s always default checks that it’s so difficult to get information that you are not privileged to have...” (REC012 CAL AB Pge5 L5-8). Nurse participants also pointed out that with current electronic records, one can follow a trail. Electronic records can easily be transferred and done so securely, making information sharing easy. Other benefits included the efficiencies derived from electronic systems such as speed of access, ease of use, and bulk access to patient information.

Electronic records curtail asking the patient the same questions by different people, foster portability, minimize transportation of paper records to different places and thus reduce potential contamination. Electronic records were described as a “one-stop-shop” for almost all patient information. One respondent remarked that “electronic” is synonymous with “availability at all times”. A participant believed that electronic records compensate for unreadable or difficult to read doctor handwriting when the participant said, “, it’s really hard to read the doctor’s handwriting, so if we could pull it up on an electronic file it would be easier...” (REC004 Pge9 L24-25). Ready access to records by specialists and not having to repeat tests, etc. was mentioned as a benefit of electronic records, and in the respondent’s own words, “...As a patient standpoint, I would like the electronic health record because then, if I go see a specialist, they have all my records from previous, no matter who I saw...” (REC013 SK Pge4 L15-17).

Although so much was said regarding the benefits and usefulness of electronic records, the nurses who were interviewed did not hesitate talking about the shortfalls of such record systems. Some of the shortfalls were, the ease with which electronic records could be easily copied or deleted remotely. The nurses mentioned that sometimes printed materials ended up with the wrong printer, revealing otherwise confidential information to an unintended recipient. Disparate (about 36 record systems at the time of the study) electronic record systems made it difficult to share between these different systems. For the nurses who struggle with the electronic age, the electronic record system could be a real challenge. A nurse commented, saying that, “...those who struggle with sort of the information age, the electronic world can be very much a challenge, it’s also a challenge in that, depending on the friendliness of the medical record system that is being utilized, there’s very user friendly systems and very non-user friendly

systems, you may miss things that have happened accidentally with a patient..." (REC008 RD AB Pge5 L5-9). There was also mention of what may be termed "bulk loss" with electronic records, to which a participant had this to say "...if a person brought a laptop home and the laptop was stolen from the car which has happened in the past, there's hundreds of thousands of documents in there, whereas when you had papers, you would only bring as much as you could carry..." (REC017 CAL AB Pge6 L30-31 to Pge7 L1-2). The same participant added that, "...but when it comes to patient care for security, paper is still I think very efficient..." (REC017 CAL AB Pge7 L5-6). Another participant talked about the learning curve associated with switching from paper records to electronic records use and had this to say, "...I spent most of my career in a paper world, and when you get used to a paper document, it's very easy to know where to go to look for the information. So, switching to electronic was a bit of a learning curve, to think differently how to access that information..." (REC008 RD AB Pge 5 L19-22). The same individual added that, "...a huge challenge with the paper document was if you worked in a facility that a patient had been in many times or had been in for a long period of time, there would literally often be volumes of paper documents..." (REC008 RD AB Pge5 L22-25).

Electronic records on screens made it easy for the prying eyes. A concerned participant said, "...One of the other struggles I see in our office is because with electronic information I often, will see people get up and leave for coffee or leave for lunch and not lock the computer. So then that access, someone else can come and look, and to me that's no different than giving my I.D. card to somebody else to say you have access to this building, although it's, to me it's worse than that, because that's confidential information that I'm leaving fully accessible..."

(REC008 RD AB Pge5 L7-12).

There were those participants who were apprehensive about electronic records as a result of news about hackers, and also the fact that technology can be disruptive and cause stress. There was also concern that electronic systems make nurses spend too much time on the computer and could frustrate them as well. Another concern was that digitization could make many records accessible with a few clicks. This meant that more damage can be done with electronic records than with paper records. Some nurses said that electronic record keeping could be time consuming. One participant made this comment after visiting another nursing unit; "... I was with her for four days in the hospital. And they do all of their charting at the computer. And the one thing I didn't like was, every time I went anywhere, they were always on the computer..."

(REC005 SK Pge8 L27-29).

5.11.3 Benefits v. Pitfalls of Paper Records

A participant commented that paper records made the nurse feel that she or he was working. Nurse participants in the study also indicated that homecare nurses who drove around with charts could unintentionally leave such charts in a client's home. Nurse participants said that they had difficulty identifying snoopers when it came to paper records. Easy access to rooms with paper records was another problem. Yet, other nurses shared one nurse's opinion that, "...Well, I think paper is harder to access, so it is probably more secure, electronics can be hacked.." (REC005S S PgKe9 l17-18). The participants added that outsiders dressed appropriately like nurses could gain easy access to the nursing floor, and charts. Some of the nurses voiced their frustrations at doctors who strayed in with street clothes. Also, the volume of records a nurse may have to handle could be overwhelming in some instances. For example, as mentioned earlier, a nurse said, "...a huge challenge with the paper document was if you worked

in a facility that a patient had been in many times or had been in for a long period of time, there would literally often be volumes of paper documents. So you didn't always have the full picture because you could have twenty pounds of paper documents locked up down in health records, and if you wanted to see that, you would have to request it, and it could take two or three days for those charts to arrive to you to access..." (REC008 RD AB Pge5 L22-28). Another participant recounted an unfortunate situation witnessed with paper records and said, "...in a previous job that I had, there were breaches of patient confidentiality when discharge instructions were given out with other people's patient stickers on them. And so those kinds of things can happen to you, and so there's a number of different ways that papers can be really problematic that way..." (REC009 RD AB L3-7). Other times, nurses found patient paper records misfiled. For example, "...where I work we still use paper records. It is an issue with privacy. I think because things can get lost, you sometimes you can find the wrong page in someone else's chart..." (REC021 SK Pge9 L26-30)

Such mentions were exemplified by a statement from one respondent that said, "...We use paper charts and we use also electronic information. So, we chart in the computer and we also chart on paper..." (REC022 RD AB Pge2 L17-19).

5.12 Theme G - AB and SK Health Regions – Patient Information System

Patient information privacy and security endeavors are important for every health region in Canada. Different health regions may be at different stages in their quest to put in place and use technology to formalize patient information privacy and security initiatives and practices. This section takes a look at the theme labeled "AB and SK Health Regions" Patient Information Systems and presents the results of the survey with regards to this theme. The study was

restricted to these two health regions. Sub-themes that would be under consideration will include similarities versus differences in AB and SK, urban versus rural settings, and resource availability versus limited resources.

In the 1980s, Calgary, AB was one of the first cities to initiate the electronic record or a Patient Information System. Since this time, patient information privacy and security regulations and laws have flourished, evolved, and continue to do so. In terms of the timelines for privacy events, the government of Canada enacted the Privacy Act, which applied to federal government institutions in 1983, and by 1995, the Alberta Freedom of Information and Protection of Privacy Act (the FOIP Act) was in full force. In 2000, the Alberta Health Information Act, which governs the collection, use, and disclosure of health information by custodians (hospitals, etc.) came into effect. Since then, several events regarding privacy laws and regulations have taken place. Among these events is the conversion of paper patient information records to electronic.

TABLE 5.4:

TIMELINE - All Acts related to Privacy and Security (used in Dissertation)

Date Enacted	Location	Acronym	Name of Act: Reference	Page(s) found in Dissertation/ Manuscript
1980	US	PPA	<i>Privacy Protection Act</i> (Westin, 2003).	45
1983	Canada	OPC	<i>Office of the Privacy Commissioner of Canada Acts, 1983</i> (OPC, 2011).	35, 36–39, 43, 45, 47, 63–64, 171–172, 263
2000	Alberta (AB)	HIA	<i>Alberta Health Information Act (HIA), 2000</i> (Government of AB, 2020),	7, 8, 10–11, 14, 18, 21, 171, 125

2000	Canada (CA)	FIPPA	<i>Freedom of Information and Protection of Privacy Act, 2000</i> (Government of Canada, 2020),	58, 171–172
2000	Canada (CA)	PIPEDA	<i>Personal Information Protection and Electronic Documents Act, 2000,</i> (Government of Canada, 2020)	47, 58, 60, 81
2003	Saskatchewan (SK)	HIPA	<i>Saskatchewan Health Information Protection Act (HIPA), 2003</i> (Government of SK, 2020),	iii, 4, 7, 18, 21, 58, 75
2004	Ontario (ON)	(PHIPA)	<i>The Personal Health Information Protection Act (PHIPA)</i>	58, 80, 172, 249

Conversion to electronic record use is at different stages. Nurse respondents noted that use of electronic records started at different time in different places. Some nurses noted that paper record use was still prominent in the era of electronic records. The nurses also said that some nursing regions have gone electronic and then gone back to paper record keeping, with many using a hybrid system, which is a combination of electronic and paper records. One common thread that run through all the health regions was the use of a hybrid system.

5.12.1 Similarities v. Differences in AB and SK

A participant said, “...and I can probably speak to other provinces that I’ve dealt with which is British Colombia, AB, SK, Manitoba, Northwest Territories and Nunavut, I think I would say, would be correct to say that all of those provinces are using what I would call a hybrid system...” (REC008 RD AB Pge6 L21-24). Each of these regions may have a different mix of paper and electronic records. There was a high likelihood of finding more electronic records versus paper records in the AB Health Authority than one would find in the Saskatchewan health regions. In Saskatchewan, a respondent told of a situation where the family

of a patient was asked to pay in order to have access to the patient's records and in her own words, "...I know we had one patient where the family, the patient had been with us for a long time, and family wanted to look at her chart, and she had given permission for the family to look at the chart, and I thought, you know I'm just going to double check with our manager cause I know they've got regulations. Well she, turned out she had to pay \$30 to look at the chart, or she had to pay some money to have access to her health records. And to me, I didn't think that was right. I figure, you know the patient's there, she has given us permission for the family to look at the chart, and I don't think that people should have to pay to access their health records..."

(REC005 SK Pge5 L7-14). There was no mention of any such situation in the Alberta region.

One nurse made a notable remark saying, "...I think in the Saskatoon Health Region the infrastructure is starting to fail and so nurses are concerned... (REC016 SK Pge11 L17-18, and L20-23). This tone of pessimism regarding patient information privacy and security could hardly be heard among the AB interviewees. There was the general feeling among the Saskatchewan participants that electronic record keeping was recent, and as a result, statements such as, "...in our Health Region, now we are just going through teaching about how to access or teach us how to get into the computer and look up the information..." (REC015 SK Pge8 L27-29)

As the interviews progressed in the AB and SK health regions, the disparities between the two regions were becoming apparent. A participant put it this way, "...our health region is a little bit behind in times compared to maybe AB or, America..." (REC002 SK Pge6 L24-25)

5.12.2 Resources v. Limited Resources

Resources for infrastructure and technology are often more available in the larger populated cities, especially one that is booming. Nurses in AB appeared to have access to several resources

with regards to ready access to patient information. For example, a respondent in the AB region said this “...I’m accessing multitudes of levels of patient information, both electronically through a central zone electronic medical records. I also will access information through the Alberta Netcare system as well as at times we will access certain documents on paper that are not available electronically; and then in my role, I have a certain level of access to the information that I can see and there’s pieces of that information that I can see throughout the entire province...” (REC008 RD AB Pge2 L14-20). A participant commended the rigor of the Alberta patient information privacy and security resources with a story; “...AB Health Services I think they have a lot of checks in place, and they strongly for example, I told you that another time there was a nurse who has worked I think for eleven years in different hospitals, who had always been going into different patients account, why or how she wasn’t caught all these years beats me though. But eventually she got caught, and they could trace at least with the computer part, they could trace her trail, you see, so the right checks... so there are so many checks, and I think AB Health does a good job” (REC012 CAL AB Pge12 L7-12 and L22-23). Similar comments were not forthcoming from the Saskatchewan interviewee group. Some participants in the Saskatoon Health Region thought that healthcare in the region was getting ignored and that patient information breaches by nurses were intentionally done to get attention.

CHAPTER VI DISCUSSION

In this section, attention will be focused on themes and sub-themes as they relate to the nurses' experiences in patient information privacy and security. Interactions between themes and sub-themes will be highlighted to explain certain outcomes as necessary. As indicated at the beginning of this research, the purpose of the research is to gain better understanding of the experiences of registered nurses (RNs) in patient information privacy and security in AB and SK health regions. Specific goals include capturing rich insights and concepts related to perceptions, feelings, reflections, thoughts, and even apprehension and comprehension regarding patient information privacy and security. These are important components of the nurse's experiences. Such insights should hopefully lead to understanding what is important or not important to RNs, ascertain specific implications, provide clues to understanding some existing behavior patterns, and to inform future research.

The primary research question was broadly stated as, "what are the experiences of medical-surgical and critical care registered nurses (RNs) as they comply with the AB *HIA*, (Government of AB, 2020a, 2020b) and the SK *HIPA* (Government of SK, 2020a, 2020b) in their day-to-day nursing practices". Other relevant questions related to the primary research question are "what meanings do nurses bring to patient information privacy and security practices?", "are nurses concerned about the expectations mandated by Health Information Acts?", "how adequate is the preparation nurses receive in the area of regulatory compliance?"

The word "experience" often denotes involvement in, participation in, observation of, and awareness of, therefore experience is also sometimes taken to mean an encounter, or to undergo an event or occurrence. In summary, experience is; "The actual living through an event... the

real life as contrasted with the ideal or imaginary ... The sum total of the conscious events which compose an individual life" (Erlich, 2008, p. 1126). Analysis and discussion of the results for the data collected for this research will be done keeping in mind the fundamental definition and understanding of "experience" portrayed above. Of importance to note is that experience as defined here could be overly simplistic. To nurses however, 'experience' usually means 'clinical practice.' The data collected and an initial analysis of it would suggest that experience in the context of this study involves a complex mix of clinical nursing practices, the consequences or results of such practices, and what one could call the "derivative" experiences due to such interactions. The analyses and discussions that follow will be done under the themes and sub-themes that were as a result of the study.

6.1 Theme A: Patient Information Protection

Patient information protection occurs when deliberate steps are taken to shield patient information from being accessed by individuals, groups, objects, and systems, except on legitimate need-to-know basis. Lack of protection may be due to system failure or failure of users to adhere to stipulated protection procedures. During the study, it was apparent that there were instances where patient information was left open on computer screens without the use of privacy sliding doors or pointing computer screens away from the public. This often unintended behaviour appeared to be careless abandonment or failure to log out of the computer as a result of responding to a pressing need. In some instances, the pagers used to call medical staff have led to serious patient information breaches. Fionda (2019), an investigative journalist, has written about a situation in BC, Canada, when patient information was exposed with simple pager calls. Such occurrences may leave the nurse wondering about the adequacy of control mechanisms

built into the nursing station, a feeling of loss due to the possibility of someone gaining access to otherwise confidential information and/or the need for the nurse to address any deficiencies in information privacy knowledge. Other thoughts that may be welling within the nurse may be attributing such lapses to poor nursing practices or lack of adherence to strict information privacy rules. Simple remedial actions such as targeted and programmed education informed by the nurses' experiences such as those mentioned above could minimize exposure of patient information. Also, it may suffice to say that, for the nurse, protection of the patient supersedes protection of the patient's information. Thus, actions that save a life would always precede those that protect information, even if it means relegating the latter to oblivion. Perhaps the solution to the lack of patient information protection is not to expect absolute adherence to information protection rules and regulation but providing practical examples of how the breach of such information have negatively impacted patients, and sometimes having the patients narrate their own stories during privacy and protection education sessions. In one instance, Braga, et al., (2018), have recorded the breach of patient information for 80,000 patients, revealing detailed information about these patients. The impact of such violations can be devastating. Davis (2020) reported that 41.4 million patient records were breached in the U.S in 2019. News of this nature can seriously undermine nurses' efforts to protect patient information and leave them demoralized.

The diagrams below provide a cursory elaboration of an earlier diagram (top diagram) that illustrated information flows for nurses, the other healthcare personnel nurses may interact with, some processes and procedure that may, together, provide a quick framework for understanding how patient information may escape the limits of confidentiality. The decisions

nurses make on a day-to-day basis concerning the use of patient information are influenced by a number of factors including Acts, policies and procedures, code of ethics, and the person of the nurse (emotions, feelings, state of mind, etc.). The context of such decisions is often the nursing process, using existing medical record systems. There may also be an active information exchange between the nurse and the patient's family and other relations, between the nurse and the doctor(s), between the nurse and the patient, and between nurses (peers). This environment may make for a complex communication network that the nurse needs to manage. There is a good chance that in such an environment, confidential information slippage may occur.

The second diagram, with the red arrows show some of the vulnerable points of patient information escape. The red arrows in this second diagram are pointing to areas in the communication network where slippages may happen.

Figure 6.1: (same as Figure 3.1) Conceptual Framework for Patient Information Flows
Interactions Between Components of Conceptual Framework That Generate a Nurse's Patient
Information Privacy and Security Experiences

Conceptual Framework for Patient Information Flows and Influences

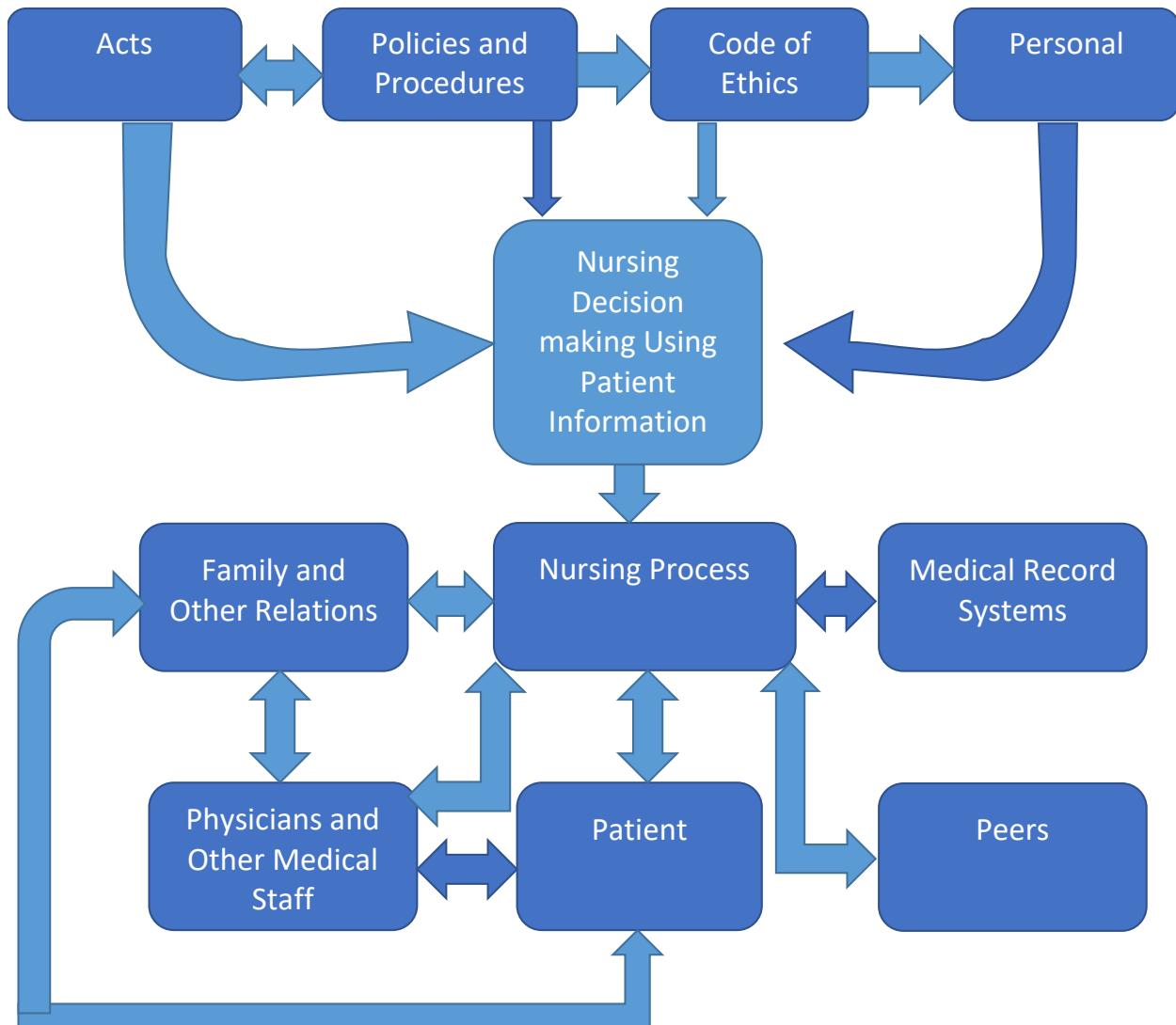
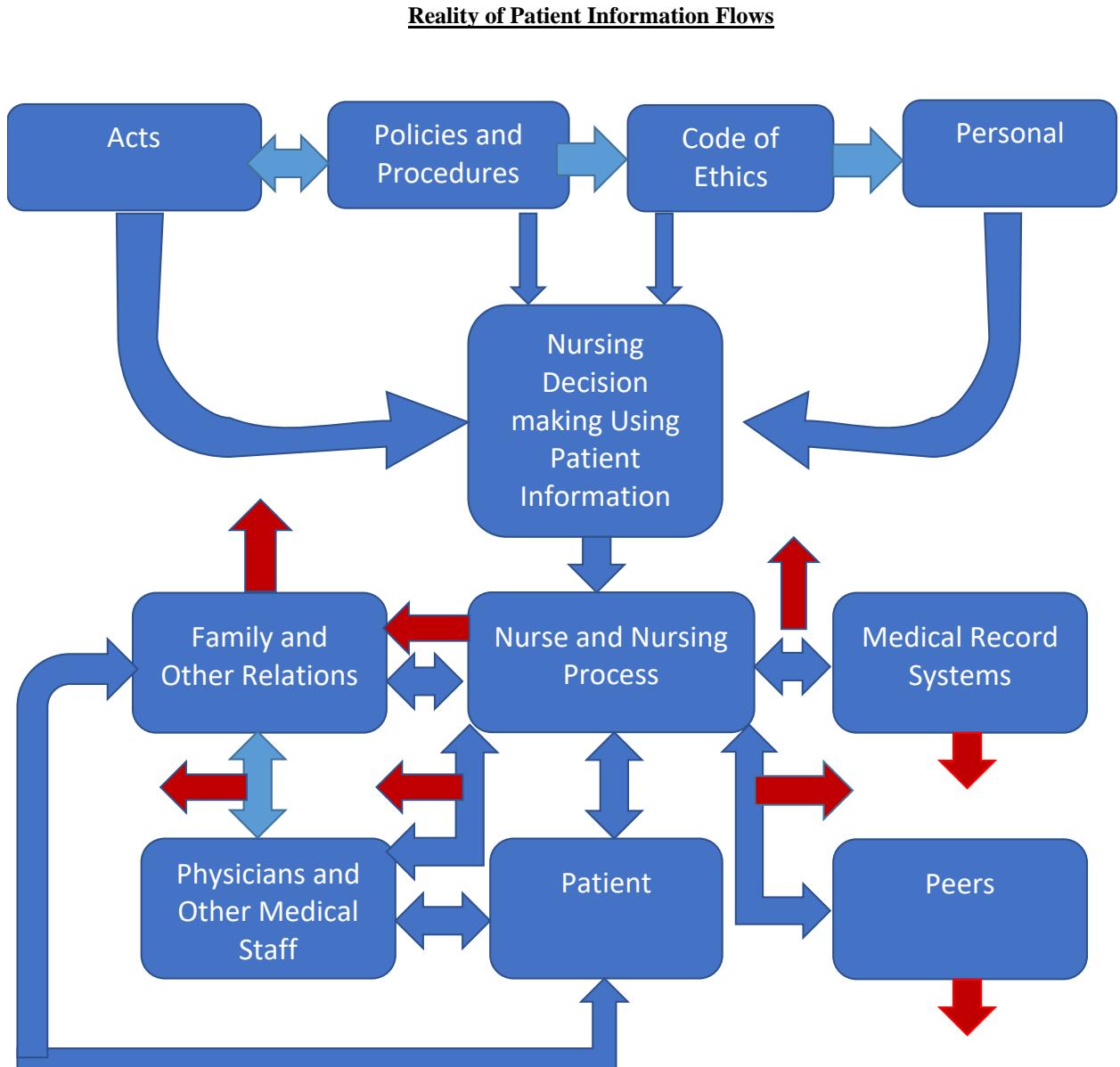


Figure 6.2: (Post Study Analysis – Reality of Patient Information Flow)

Interactions Between Components of Conceptual Framework That Generate a Nurse's Patient Information Privacy and Security Experiences



Red Arrow: Points of patient information flow (leakage) that often lead to intentional and unintentional breaches. Arrow-on-arrow indicate patient information leakages through the communication system.

In the next few sections, I analyze and discuss sub-themes that emerged from the “patient information protection” theme including protection initiatives, intentional versus unintentional protection, respect for patient information protection, safety of patient information, privacy expectations versus realities, and regulatory compliance versus interpretation.

6.1.1 Sub-Theme: Protection Initiatives

As in most endeavors, soliciting commitment from nurses involved in making patient information privacy and security a reality could yield many positive results. During the interviewing, some nurses indicated that in some situations, nurses were asked early in their employment process to sign an affidavit not to engage in certain unsafe practices. While they did not indicate the details of the affidavit, it may be reasonable to assume that signed commitments are likely to be taken seriously by the nurses. This method of ensuring commitment is proactive and creates awareness of the importance of patient information privacy, and indicates the willingness and involvement of the nurse. The data did not clarify whether signing of an affidavit was pervasive or limited, or whether it is producing desired results. Although the signing of an affidavit is a useful initiative, it may not be sufficient in the long term. Signing an affidavit has the tendency to have some nurses believe that once they have legally obliged, they may not necessarily have to be ethical in their decision-making. Baltzan (2019) has provided a model for decision making involving legal and ethical considerations. He proposes four possibilities where legal and ethical decisions intersect: legal and ethical, illegal but ethical, legal but unethical, and illegal and unethical. Baltzan has suggested that ethics are critical in operating a successful business today, and admonishes that a business should never find itself being illegal and

unethical. A nurse would likely want to be legal and ethical. An affidavit may provide for legal compliance, but the ethical component may still be in the hands of the nurse.

Other protection initiatives included misinforming (lying) to conceal a patient's identity, not allowing names on worksheets for confidential patients, and finding alternative ways to identify confidential patients. The nurse's readiness to even misinform (lie) to protect privacy is significant. This is a confirmation of the nurse's commitment and importance of respecting the patient's information privacy. Also, not allowing names on worksheets and finding alternatives to identifying confidential patients were tangible steps taken by the nurse to protect the patient's information. The foregoing discussion would suggest that the nurse would literally do "anything" to protect privacy. The nurse's commitment to protect the patient's information should be applauded. However, should this be done at all costs, including "distortion of the truth" – lying? Allowing this kind of behaviour could encourage other forms of behaviours that may question the integrity of the nurse. Misinforming or lying in the instance described above is a depiction of a desperate move to demonstrate commitment.

6.1.2 Sub-Theme: Intentional v. Unintentional

In order to be intentional, the nurse would have to be deliberate about protecting the patient's information. Results of the study showed that being intentional about respecting the patient's information was necessary for protecting it. Showing respect for the patient by respecting patient information confidentiality, could be synonymous with honouring the patient, and this honour, when acknowledged by the patient can produce a feeling of accomplishment and satisfaction for the nurse. Also of importance was that the nurse was intentional about not sharing patient information unless absolutely necessary as part of their treatment plan. As sharing

has almost become very much part of relationships, it is not uncommon to find individuals intuitively sharing what they did not intend to. Being intentional here suggests for nurses to exert some level of effort and exercise self-control when it comes to patient information privacy. Patient information privacy needs to be treated as an ethical (PI and ethics) duty and for that matter, nurses need to follow rules (nursing culture that promotes PI confidentiality). Regardless of temperament, the nurse would have to learn to exercise discreetness. This active protection process for assuring confidentiality indicates the determination to protect patient information. In the end, the nurse is likely to experience a good sense of being a valued custodian, ready and willing to observe due diligence when it comes to patient information privacy. The wrong perception may be that a long list of “to-do” or “not-to-do list” is being made for the already busy nurse. Quite ironically, the need for the nurse to be intentional stems partly from the nurse’s busy and unpredictable work environment. This need to be intentional may be particularly important for new nurses who are in the process of making nursing practices part of who they are. Over time, these practices may become intuitive but not for a protracted period of time due to the dynamic nature of the nurse’s environment.

6.1.3 Sub-Theme: Safety

Safety in the context of this discussion refers to how to combat events and situations that could adversely impact the privacy of patient information. Regarding safety, the nurses that were interviewed were asked to consider what could happen to data while in transmission. Data in transmission could end up in the wrong hands, could be hacked, or altered, leading to compromise of the data’s integrity, making the patient information unreliable. Proximity of other patients was another safety issue. In a number of cases, it was easy for patients to over-hear what

was being said about other patients. The nurses that were interviewed said workstations were at times unlocked and open, allowing anyone close by to see what is displayed on the computer screen. Physical placement of nursing stations was also a concern. In a study that examined the role of visibility and proximity on, among other things, perception of privacy, Xiaoding et al. (2019), concluded that privacy was one of the important considerations in the design of nursing stations. Bedside reporting in shared rooms and physical placement of nursing stations was an issue that needed to be dealt with. The above conditions surrounding the nurses' work environment called for the nurses to actively protect patient information by being alert, aware, and conscious of their "vulnerable" surroundings as they carried out their primary responsibility of caring for the patient.

While the nurses that were interviewed acknowledged the importance of ensuring safety, they also expressed their personal experiences regarding privacy expectations. There were those who felt that the privacy expectations imputed on them were unrealistic, considering that they have no control over the work environment and that their primary focus is the patient's well-being. The interviewees also made it clear that it is never going to be completely private (privacy and how the nurse feels about it). This was not to be confused with intentional defiance of privacy mandates but an expression of what the nurse's reality was. What this reality looks like for the nurse is difficult to tell, and also, how this reality manifests may be different for different nurses or groups. The nurses respected regulatory compliance, with some even advocating for what they called "privacy for comfort", which according to a nurse, meant working hard to maintain privacy to the point that the patient would not have to worry about privacy breach and to have the peace of mind to focus on recovery.

Although it is not difficult to understand that the challenges the nurses were dealing with were not of their making, it was also demonstrably clear to me, the interviewer that the participants were not complaining about the nature of their work or its environment. They were just being upfront with what they dealt with on a day-to-day basis. The concerns mentioned here may be what the nursing administrators' list of challenges are to overcome. Given the restraining work environment and the myriad of expectations nurses have to deal with, one could readily sense the depth of the nurses' responsibilities and even sympathize with them. If the nurse had to choose between the safety of the patient and the safety of the patient's information, the choice would be obvious.

6.1.4 Sub-Theme: Expectations v. Realities

Expectation as used in this discussion has three dimensions. First, expectations by way of standards the nurse has set for herself or himself as a result of personal principles and/or in combination with professional code of conduct such as the nurses' code of ethics. The second expectation pertains to peer assessment of the nurse's professional conduct, which essentially has to do with what nurses think of each other. This kind of expectation measures how fellow nurses measure the performance of another nurse. Thirdly, we will look at expectations that come from the authorities. Data collected during the research indicated that nurses are generally in compliance with regulations and respect that law. In an article entitled "A Nurse's Guide to the Use of Social Media" (NCSBN, 2018), has provided several of what the organization calls "Common Myths and Misunderstandings of Social Media" to indicate that most disclosures by nurses are unintentional. These myths and misunderstandings have contributed to a nurse's inadvertently violating patient privacy and confidentiality while using social media. Same data

collected during the study showed that nurses understood privacy and take it seriously. Important to note is that nurses may have to deal with the expectations individually or in groups. These expectations may include knowing and complying with the dictates of professional principles, being a cardinal member of the life-saving team, and someone who can be trusted. These expectations could bring significant pressure to bear on the nurse. While nurses have these expectations to deal with, they also have their personal realities. In some instances, nurses have to choose between pleasing the many observers by conforming to expectations or satisfy personal emotions and do as he or she pleases. Such strong emotions may explain why few, but some nurses go ahead and incessantly post patient information on social media platforms in spite of all the expectations and apprehension by other nurses. The nurses interviewed made mention of the reality of their own humanity, and how they are likely to “slip” here and there over time. One would not find it difficult to deduce from their actions and body language that in the nurse’s experience, given expectations and the reality, reality is more likely to trump. The nurses, by their deeds and actions were advocating for both the reality and reasonable expectations, in other words, realistic expectations.

The College of Registered Nurses of Manitoba (2020), has indicated that nurses have the responsibility to identify issues that could negatively impact the nurses’ ability to practice according to the College’s regulations, practice directions, Code of Ethics, and other provincial and federal legislation. This shows how important compliance is to the nurses, and yet, how overwhelming the nurses’ responsibilities could be.

6.1.5 Sub-Theme: Regulatory Compliance v. Interpretation

Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business processes. Interpretation on the other hand is the action of explaining the meaning of something. The nurses that were interviewed understood the essence of regulatory compliance, which is protection of patient information. They however pointed out that the same regulation may mean different things to different nurses, particularly, the younger nurses. There were no filters to run a nurse's interpretation of the elements of where they need to be compliant. Thus, the meaning of a nurse's actions concerning regulatory compliance was for the most part "at the mercy of the nurse". Some of the interviewees indicated their conscious awareness of this situation and indicated that, as at the time of the interviews, they had no formal forums to discuss such concerns. In the absence of such avenues for discussions and reform, many would resort to "elevator" and "lunch room" informal unplanned meetings for discussions.

While nurses learned from each other the right things to do at these meetings, there is the tendency for misinformation leading to aggravation or compounding of errors. As the nurses voiced some of these complaints, it was not difficult to perceive their frustrations as some felt "caught between a rock and a hard place". The fundamental question one would ask in this situation is whether it is better for the nurses not to talk to each other and make "fatal" mistakes or share their concerns with their peers, get help and possibly save a life. Although the response to a question of this nature might appear to be obvious, one needs to exercise caution and not draw quick conclusions, as this issue may be contentious and/or debatable.

Other concerns the nurses had regarding regulatory compliance included the language the regulations were written in. Often, the laws, regulations, policies, etc. that form the basis for regulatory compliance are written by, or under the guidance of legal practitioners sometimes

using language only trained lawyers could fully understand. As a result, a nurse may read a regulation or policy and not fully comprehend the meaning of what the regulation is requiring the nurse to do. Instances like this could lead to honest mistakes by the nurse. Such mistakes, often preventable, can be costly. Remedies for shortcomings of this nature could be planned educational programs. Orientation of nurses did not come up as a topic for discussion during the interviewing process. One would expect that important policies and regulations will be explained in plain language, particularly for new nurses and the process repeated whenever there are updates to these policies and regulations. There was also no indication at the time of interviewing that administrative processes were in place to encourage nurses to be forthcoming with their concerns regarding regulatory compliance. What was apparent in the course of the interviews was that the nurses needed a resolution for minimizing the possibility of misinterpretation of regulations and sometimes clearly verbalized their frustrations.

The nurses also derided the thinking that regulations were not followed due to lack of knowledge or understanding, an experience which can be quite humbling for the nurse. During the study, it became important that “knowledge and understanding” is not confused with “subjective interpretation” of the rules to be followed. The rigor of a nurse’s education perhaps makes him or her adept to the point of sometimes reading too much into situations. They would rather be safe than sorry.

Another experience the nurses shared was the feeling that regulations were often cumbersome and “in the way”. In an article published in the magazine Minority Nurse, Phillips (2020) mentions that, as nurses, they may be “challenged” to stay abreast on the many new state laws that may impact the health of those that reside in their immediate communities. She goes on

to write that, for example, beginning January 1, 2020, two hundred and fifty-five new laws will take effect in Illinois. The author adds that nurses may need to familiarize themselves with the new laws and regulations. She goes on and further writes that locating such information could be laborious, unless efforts are made to compile the information and make it available to the nurses. The nurses insinuated that sometimes they had practical and better solutions for patient care that were not necessarily compliant. In such instances, they felt their hands were tied by laws and regulations. In the nurse's experience, there is considerable bureaucracy in the discharge of his or duties. There was a rather strong preference for common sense by the nurse. In the estimation of some of the nurses that were interviewed, nurses conform to regulations more out of fear than personal conviction, an experience which some hoped could be altered.

There were also those nurses that felt that regulations are not impediments but imperative. The dilemma of the nurse when making sometimes critical decisions is choosing between a nurse's many years of experience or policies and regulation some of which may even need updating. The reality again is that there are no easy answers. Difficult questions to answer would include how to categorize the many patient information policies and regulations into levels of importance and prescribing how to deal with the different levels. The danger with categorizing and labeling is the tendency to put undue focus on what has been labeled "important" and ignoring everything else to the detriment of the entire system.

6.2 Theme B: Patient Information Breach

A breach is the breaking of a rule or law or the upsetting of a normal and desired state. Information privacy breach could therefore be defined as any act that is contrary to established information privacy laws, rules, regulations, standards, and similar mandates designed to protect

information privacy. In this section, several sub-themes that emerged under the theme “Patient Information Breach” are analyzed and discussed.

6.2.1 Sub-Theme: Intentional v. Unintentional Breaches

Nurses are aware that checking on patient information that does not help to provide care is a breach. The nurses that were interviewed indicated that some nurses have the habit of intentionally accessing their neighbour’s or other nurses’ records. They even sometimes access their own health records. Although such access to patient information is often intentional, many are not meant to be malicious. This level of seemingly unrestrained access that has almost become a commonplace could be attributed to shortfalls in access control. Nursing managers or administrators in consultation with the nurses could collaborate in finding a resolution that would not hamper the nurse’s duties and at the same time minimize the infraction described above. This would be a critical balancing act. The individual who is not part of the nurse’s day-to-day grind may be tempted to suggest that since the act being described here is intentional, all the nurse needs to do to eliminate this issue is exercise self-control. Although this may be a reasonable suggestion, it should be kept in mind that once habits are formed, they may be difficult to break. There is no doubt that something needs to be done to correct the situation, but it needs to be done with care and further investigation. Sometimes unintentional breaches occurred as nurses shared unusual experiences on Facebook with their friends and family. Unintentional breaches also occurred during coffee room chats and lunch-room talks. There were also instances when nurses have left reminder notes on counters, med rooms, or the notes themselves have fallen to the floor. Nurses often held conversations about their patients in the hallway. Perhaps, the nurses also need what may be termed “un-programmed Facetime” where certain rooms may be

dedicated to unplanned meetings for brief moments for consultation with designated experienced nurses.

Certain behaviors are as a result of human tendencies and could be extremely difficult to overcome. Many of the unintentional behaviors described above are human tendencies. The solution to how they should be dealt with could be the subject of further investigation. There are no easy answers. While some privacy violations were as a result of concern for certain individuals, other violations were just to pry. There were several reasons suggested for intentional breaches including lack of morality on the part of the nurses who cannot exercise restraint. In some cases, nurses violated the rules to portray some emotional feelings towards unresolved issues and to bring about change. Other motives for intentional breaches were strong feelings about drawing public attention to concerns the nurses have. Apprehension was also identified as a reason for deliberate breaches. In the nurses' opinion, these individuals break the rules to redress inequities of one form or another. The many breaches could also be as a result of loss of control of nursing practice behaviours. Of importance is that nursing administrators and authorities not turn a blind eye to the many experiences the nurses have revealed. Some of the concerns may warrant further investigation requiring action. Controlling patient information privacy from the nurse's perspective would involve controlling two main areas, access to the patient's information and divulging of same information once accessed.

6.2.2 Sub-Theme: Attitudes Towards Breach

Understanding the attitudes nurses have about breaches could help determine possible solutions for dealing with the issue of breach. The attitudes nurses have about breaches could provide some indication of how important breach is to patient information privacy and security.

6.2.2.1 Seriousness. Some of the nurses indicated that patient information breach is not taken seriously by the nursing community and even suggested that breaching would continue in perpetuity. According to those who have this mindset, patient information privacy is not in the forefront enough. In response to this, one would argue that drawing attention to patient information privacy as it relates to nurses could be a sensitive issue. Nurses may react to this attention in a manner that may not be in the best interest of the patient. This is not by any means suggesting that nurses will act mischievously to restrictions. Strict conformance to the rules may not leave room for the nurse to exercise professional judgement calls when it came to choosing between the rules and the best interest of the patient.

6.2.2.2 Consequences. The nurses also indicated that consequences of patient information breach are also often not clear and therefore, breaches are not likely to be taken seriously. Here, perhaps the nurses are asking for a clear categorization of breaches and the punitive consequences associated with the categories. The nurses are also implicitly saying that until nurses see on a consistent basis how violators are dealt with, there will be no deterrents to information breaches. This approach would probably produce the same response as nurses not taking breaches seriously.

6.2.2.3 Sharing. There was also the thinking by some that sharing is the second nature of the nurse and implied that as a result, breaches will be difficult to stop. This admittance sounds disturbing and hopeless on the surface. However, the incessant sharing habit that some claim has

come to stay with nurses may have some inherent benefits that could be leveraged by a well thought out study of the current sharing processes to understand how they work, take necessary intervention steps, and introduce some level of control. If properly done, it could translate the current “illegitimate sharing” to a formal and legitimate forum for critical information exchange.

6.2.2.4 Saying Too Much. The nurses also alluded that sometimes nurses say too much about patients in their care. This behaviour is likely to encourage breaches. This could be perceived as extension of the sharing habit. The question is whether the nurses are aware that the barrage of information released about their patients include some trespassing. As indicated earlier, nurses have also questioned the adequacy of the consequences for breaches. If the consequences are not serious, then breaches may not be such a big deal as the personal benefits of breaching may far outweigh the consequences. Therefore, there will be little motivation to stop this practice.

6.2.2.5 Hesitation to Report. The nurses indicated that there were some situations where they simply did not know how to deal with, such as when another nurse is observed looking up files for a patient not in the nurse’s care. In such situations, one could quickly suggest reporting to the authorities. Perhaps the hesitation to report such incidences stems from the pervasiveness of such practices. The nurse who is observing such a behavior would agree that he or she is not exempt from this behavior. The reality however is that such behaviours may be a web of complex inter-relationships that may over-shadow the need for principled work life.

6.2.2.6 Famous Person Situation: Breaches More Likely. The nurses shared what I would like to call a weakness, the idea of the assurance that information for any famous person was more likely going to be breached. Some nurses shared their attempts to help stop breaches

by fellow nurses but have been frustrated by the persistent breaches, and their temptation to go with the “if you can’t beat them, join them” attitude.

6.2.2.7 Willingness to Share Challenges. The nurses’ willingness to share their challenges in patient information privacy was very encouraging. The opinion of the writer is that rather than rush to fallacious conclusions about how the nurses ought to be punished for sharing the reality of what they have to deal with, “all hands will be on deck” helping to reduce contentions so nurses would be free to do what they love to do best, being there for their patients. The experiences nurses have shared regarding their attitudes towards breaches should serve as a guide to understanding why and how breaches occur, and to some extent, how to deal with breaches.

6.2.3 Sub-Theme: Why Breaches Occur

The nurses indicated there were a number of reasons breaches occurred. The causes of the breaches the nurses enumerated included curiosity, entertainment, human nature, pressure from patient’s family, boredom, lack of education, reaction or response from fellow nurses and others, and action or inaction on the part of the nurse. The next few paragraphs take a closer look at the nurses’ narrations and discuss each of the reasons the nurses provided for the occurrence of breaches. A closer look at the nurses’ narrations provide a discussion point for each of the reasons the nurses give for the occurrence of breaches.

6.2.3.1 Curiosity. The nurses indicated that curiosity was a major part of why breaches were happening. In some cases, a patient may be of interest to a nurse. This patient may be an acquaintance or may be on a “chain of relations”. The nurse would like to know what brought the acquaintance to the hospital and in some cases, possibly find out how they could help. On a

number of occasions, the nurse is seeking to merely inform himself or herself and satisfy the desire to know. Another major reason, according to the nurses, that may cause an almost inevitable breach with regards to curiosity was when a notable public figure was in the hospital. Nurses were curious to know what brought this individual to the hospital. In all these instances, a breach occurred as the nurse accessed information about a patient not in his or her care. A breach can also occur as the nurse who is providing care divulges the patient's information to another nurse. The argument could be made for the possibility of the patient whose information is improperly accessed coming under the care of the nurse at some point in time. What would be the difference if the patient's information was accessed then or now? What would the differences be if the patient's information was accessed legitimately or out of curiosity? Ultimately, how that information is used should even be more concerning. Therefore, there needs to be a balanced approach to how one perceives a nurses' access to patient information. The truth could be said that, after all, the better the nurses are informed, the better care they are able to provide or the more responsive the nurse could be. On the contrary, encouraging such arbitrary access and dissemination of patient information would result in a web of information flows that could be extremely complex to control. Information sought for the purpose of resolving a problem has value and may eventually translate to knowledge. Information acquired or obtained just for the sake of knowing, may be referred to as idle information and may be inappropriately shared, leading to even more breaches. Would it appear that curiosity, as it is often said, is an act of human nature and thus should be excusable?

6.2.3.2 Human Nature. Some nurses argued that nurses are human and have human tendencies such as the desire to know, do, share, and in some cases may have compulsive

behaviors that may lead to breaches. The reality is that the nurses who may be engaging in such compulsive behaviours may not even realize the seriousness of it or may even down-play the situation, particularly if other nurses are enjoying the perceived humour.

6.2.3.3 Entertainment. Sometimes some nurses may find the patient's condition humorous or entertaining and may even want to share with others and in some instances make such information public. Although most of the nurses that were interviewed frowned at this, others may actively be seeking opportunities to see or post what may be called "funny pictures" such as taking pictures of sleeping patients and making fun of them or posting these pictures on social media.

6.2.3.4 Pressure from Patient's Family. A major reason for the breaches that occurred was pressure from the patient's family. Family members came in or called to demand information about a patient and did so with impunity, as if they had the right to such information. According to the nurses who were interviewed, often the calls and visits were so rampant that sometimes the nurses felt that the family members were evading the nurse's space. The pressure nurses felt was intensified as they perceived the frustrations from the patient's family members, for whatever reason, frequently directed at them. Perhaps the nursing authorities need to pay attention to nurse-patient family relations and establish a protocol that would provide family members the feeling of empowerment as they participate in the patient's care. Nurses could leverage the care family members have for the patient in such a manner that it becomes a win-win situation for the nurse as well as the patient's family member.

The nurses acknowledged that interruptions could take attention from patient care, particularly for issues that needed resolution sooner than later. Repercussions for continued

pressure could be compromises on the part of the nurse and loss of attention to the patient as the nurse becomes agitated.

6.2.3.5 Boredom. Contrary to the busyness brought about by the patient's family, the nurses admitted that the spurts of downtime (i.e., night shift) got them bored with little to do. They would sometimes resort to surfing the information system they work with, like they would the internet, snooping for information. The nurses added that they would snoop to break the boredom while satisfying the desire to get interesting information.

6.2.3.6 Lack of Education. The nurses mentioned that lack of education may explain the level of breaches witnessed today. They wished there was more education directed at the protection and enforcement of patient information privacy. Continual education is particularly important as the political-legal environment of patient information privacy and security may be in a state of constant flux. Nurses need to be informed and updated in a principled and planned manner only education can provide. Some of the nurses said that educational institutions they attended had high expectations for information confidentiality. As a result of the perceived deficiency in privacy education, nurses were under pressure to self-educate in privacy matters. According to the nurses, the absence of this education would perpetuate the perceived knowledge gap. Perhaps, nursing managers and authorities could incentivize the nurses' desire to self-educate when it comes to patient information privacy and security in an attempt to promote education in this area.

6.2.3.7 Reaction v. Response. A breach may be an intentional act to draw attention to an existing issue or issues not receiving the needed attention or get a response from the nursing community. Such reaction or response by angry nurses may be all that is needed to resolve a

long-standing issue. Intentional breaches may be seen by other nurses who may not normally condone such acts as desperate steps for much needed answers. A simple hypothetical example may illustrate how intentional breaches could be used to redress an existing issue. During the study, there was mention that certain nursing practices were revealing of patient information, such as having patient names on charts and paper records. If nurses have requested the patient's name to be removed from the front of the charts and paper records and they felt that the authorities were oblivious to their request, nurses could intentionally leave the charts and paper records on desks unattended to. This act may lead to complaints by other parties that would get the attention of the authorities. This act of defiance is analogous with the current civil disobedience by individuals clamoring for the end to the stay-at-home lockdown as a result of the novel coronavirus pandemic. The danger with authorities giving in to such actions is the possibility of future actions by nurses that might threaten the very lives of the patients the nurses are supposed to care for. In other words, the authorities should find ways of not succumbing to uprising by the nurses.

6.2.3.8 Action v. Inaction. Actions and inactions by nurses were also considered when it came to gaining some insights to why breaches occurred. Actions and inactions by nurses are a broad category of what the nurses do or do not do that affect patient information privacy and security. According to the nurses, actions included the nurse texting patient information to colleagues in another facility. While the nurses did not always provide detailed reasons for such acts, it may be reasonable to surmise that they may be seeking help from fellow nurses for some desperate life and death situations they may be facing. Those who are quick to judge or criticize need to note that in such situations, privacy, confidentiality, security, and other information protection may

not matter. The nurse's focus would be to do what she or he was hired to do, save lives. The important thing here is to ascertain if the nurse is aware and can follow existing protocols while saving a life. Texting patient information to colleagues in another facility may just be a blatant act of breaching privacy, such as sending humorous patient information as discussed before. Other actions included nurses deliberately and inappropriately accessing information about other nurses, nurses viewing the charts of other nurses on admission, and accessing their own records. Many of these breaching acts did not have easy answers to the deeper rationale for such acts.

My personal observations during the study was that it appeared as if no one is even watching. Unintentional acts such as leaving printed electronic materials on desks easily accessible by others was a problem as well as conversations between colleagues in public places. Sometimes it may appear that since names are not mentioned, the conversation is private, but one could imagine himself or herself as the patient's acquaintance fully aware of what the elevator conversation is about. What feelings would hearing such conversations bring? The nurses pointed out that sometimes emergency calls caused them to leave patients in the open in attempts to promptly respond to such calls. The contention one would raise is that if patient information is as important to the "powers that be", a protocol would by now have been established, as the two actions of responding to emergency calls and ensuring protection of patient information are not mutually exclusive.

6.2.3.9 Venting. Venting appears to be therapeutic in certain situations. Some nurses confessed that after a hard day's work, off-loading some of the workplace frustrations could be refreshing. There was some indication that venting to family members at home occurred among the nurses. However, venting may include narrating workplace incidents or frustrations that may

have happened, and sometimes not withholding intimate details about patients. A nurse would also call another colleague who understands and could empathize with her or him and share details about a patient that can be quite revealing. Here, the intent is often not to divulge the patient's personal information but the emotions that sometimes may come with venting may cause the venting nurse to overlook what information is being shared. Again, there are no easy answers to such situations. Perhaps, further investigation into this area is needed to provide avenues for appropriately dealing with such issues.

6.3 Theme C: Access to Patient Information

In the course of data collection, it became apparent by the nurses that they receive a lot more information than needed for treatment. The natural reaction to the abundance of patient information is to try and control the volume of information coming from the patients. Having said this, it is however important that steps are not taken to restrain patients from passing on information. Medical practitioners including physicians and nurses need information from the patients for proper diagnosis and treatment. Other forms of information that may be needed include: allergies, age, past medical and mental health and addiction history. Attempts to stop or limit the free flow of information between patients and nurses could lead to misdiagnosis and even become dangerous. Thus, the more information nurses get from patients, the better their diagnosis and treatment. The big question then is, "how should nurses treat excessive information provided by patients?" While I would not pretend to have answers to such questions, educating and training nurses to be "sifters" of patient information appears to be one plausible solution. This could be something the nurses naturally have to do.

Another avenue for perpetrating patient information protection is through the electronic records system. This record system affords the nurses ready availability to patient information with the benefit of expedited diagnosis and treatment. As with the suggested control of information flow between the nurse and patient, the interaction between the nurse and recorded patient information needs to be controlled accordingly. While more information may be better than less, much of irrelevant or redundant information could lead to the nurse missing important details. As the repository of data becomes heavy with what may be considered to be unimportant information, filtering of such loaded databases may be unnecessarily prolonged. The consequences may be deleterious to the patient. The ability of a nurse to collect the appropriate level of patient information should come with the nurse's experience.

Results of the interviews conducted also revealed that there have been instances where nurses have intentionally posted to public platforms such as Facebook. Suggesting that such actions be punished overtly in order to deter behaviours of this nature may not be considered over-reaction. A couple of nurses indicated that there had been instances where they had to report a nurse who posted patient information on the internet to authorities. Some kind of an explicit informal peer observation program among the nurses may deter posting of patient information to social media platforms. This is likely to gain momentum among nurses as a great majority of nurses understand that it is their responsibility to protect patient information. As was clearly demonstrated during the data collection, nurses know that they are in a position of trust and sometimes confidants especially for patients who do not have family. Role-based access control may have to be accentuated and strictly enforced to limit access as a matter of due diligence.

There was mention by the nurses who participated in the study that professional regulations were critical to maintaining privacy. The obvious question one may ask is, if the concerns and mechanisms for curtailing evasion of patient information are real, why do breaches continue? The answer to this question may seem to be simply a lack of intensive monitoring and ensuring that corrective actions are taken by the appropriate individuals. However, monitoring, depending on how it is done, could be misinterpreted as intrusion of the nurse's space or even "witch hunting". This may subsequently lead to nurses beginning to conceal actions and other unhealthy workplace practices.

In addition to knowing, respecting, and following regulations, nurses need to be actively involved in the search for workable resolutions to some of the concerns enumerated above. Fist-waving in the faces of highly trained professionals such as nurses in attempts to "coerce into compliance" often does not produce the desired results. Nurses believed that professional behaviour is important but not always pragmatic and sometimes frustrating. Some nurses expressed the frustration of not being able to share in order to learn.

6.3.1 Sub-Theme: Sharing Information v. Protection of Information

Although not sharing patient information may result in protecting that information, it is important to note that "not sharing" is not equivalent to "protecting". While sharing is often discretionary and gives the subject the option to make a choice, protection is an act that leaves no choice and must be done. Therefore, there are several regulations, policies, mandates, etc. that nurses must comply with to ensure protection. Dealing with sharing, whether peer, private, or public would appear to be more challenging than enforcing protection. Protection would often

come with stipulations to be followed while sharing can be subjective. Protection and sharing deserve significant attention, but more so sharing than protection for the reasons stated above.

In line with sharing, Clark (2020) has indicated in an article about real-world examples of social media HIPAA violations that, in the first half of 2018, more than 56% of the 4.5 billion compromised data records were from social media incidents. She went on to write that some of these were HIPAA violations from employees posting a patient's protected health information (PHI) on the social web. The author also wrote about the apprehension associated with sharing patient information online, adding that yet, employees still share patient information. The last bit of Clark's sentiments validates what some of the study subjects believed, that, perhaps, patient information sharing by nurses may continue in perpetuity.

Another dimension of sharing equally disturbing was sharing of system login information such as passwords. This type of peer sharing facilitated ready access to patient information, similar to sharing the patient's information but on a much larger scale. Such access to login information could open the door to volumes of patient information, especially if this access information is for another autonomous system. This would expand the scope of access for a nurse engaged in system information sharing.

The data collected for this study are not intended to help prescribe solutions to lapses in patient information privacy. However, sometimes what is effortlessly learned from the data could provide easy solutions. For example, during data collection, I learned that some nurses generally appreciated the privilege of the nurse chosen as a confidant with whom the patient shares personal information. This affirmation could be used to encourage and nurture a trust relationship between nurses and patients that would eventually lead to the nurse's personal

conviction to protect patient information. Decisions made as a result of personal conviction are likely to produce desired results.

In the study, fellow nurses were appealing to other nurses to be intentional about protecting patient information. As the trust relationship between the nurse and the patient develops to the point of the patient sharing personal information not related to treatment, the patient becomes voluntarily further exposed if the nurse is not trained to exercise self-restraint. On the subject of protecting patient information, the nurses appeared to be split on whether paper or electronic record systems provide better protection. Each of these systems has its strengths and weaknesses.

6.3.2 Sub-Theme: Social Media

Sharing information on social media has become pervasive in every endeavor of work and personal life, including nursing. The platform for sharing has also become indiscriminate.

Among the popular platforms are Facebook, Facetime, Twitter, Whatsapp and Zoom. The interviewees alluded that younger nurses have a higher tendency to post to a social network. This generation of younger nurses get excited about first time nursing experiences and would often want to share. Some nurses believed that posting patient information without explicitly divulging the patient's personal information that reveal the patient's identity is acceptable. Perhaps, providing the nurses a forum to safely share personal first-time experiences and to learn from them needs to be explored. Orientation programs for new nurses need to emphasize privacy compliance with practical examples and what the consequences of previous violations have been. The seriousness and non-tolerance for sharing patient information on social media should be

made clear to the nurses even if this means publicizing violations and their consequences in nursing media in order to bring attention to the importance of not sharing patient information.

Some nurses voiced that some of the sharing that occurred was as a result of venting. As nurses share especially negative work experiences with particularly close relations in frustration, little care is taken to guard against letting out confidential information about a patient.

There was also indication that if some nurses found a patient's situation humorous, it is likely to be shared on social media, at times in graphic details. Such acts could be considered impulsive and should be discouraged. As some of the nurses rightly pointed out, a nurse is a well-trained professional who needs to be disciplined and exercise self-control. Again, the message of non-tolerance should be conveyed to all.

The part of social media sharing I found strange and yet intriguing was when a few nurses said that for a number of nurses, nursing is a life-long journey and found sharing on social media as a way of reporting or journaling events and occurrences on this life-long adventure. This way of sharing may be psychological and have some emotional implications that may need more than regulatory compliance to deal with. Even more puzzling was nurses who were obsessed with sharing what one nurse termed "crazy" events that have happened to them as nurses. Some nurses indicated that the social media platform was a chance to be heard. If there were issues the nurses considered important and needed resolution but do not feel the authorities are paying attention to, they considered blatant publication of the issue on social media to get the attention of the powers that be. I however found no evidence that this tactic worked. Perhaps, further investigation of this matter is warranted.

6.4 Theme D: Education of Patient Information

Education is often used in several ways to achieve different goals. In this study, nurses understood that education was used as a tool to inform. Education is not only formally used to inform an organization's employees but also to re-orient ways of thinking in a particular direction. The purpose of such information was to bring awareness that would alert nurses to take the necessary steps to minimize or even prevent breach of patient information privacy. The significance of education in fostering patient information privacy and security can therefore not be over-emphasized.

Awareness of patient information privacy for the nurse, as they indicated during interviewing started early in nursing school. Once the nursing student becomes a nursing professional, patient information privacy knowledge acquired while in nursing school was reinforced by mandatory ongoing professional development training programs designed to update and further inform the nurse. Nurses did not need much convincing about the importance and significance of maintaining privacy and confidentiality of patient information, as many regarded this as an obligation. While using incidents of breaches as training opportunities is in order, there was little indication of the intensity of preventative training when it came to patient information privacy. A study on breach incidents and training could shed more light on whether training programs are producing the desired results. During such training, it may appear that technical details may not be necessary, but as one nurse expressed, shedding light on one capability of the monitoring systems such as the ability to audit or forensically retrieve a nurse's access to records in the system may be all that is needed to deter inappropriate access to patient information.

The ability to or difficulty with connecting theory with reality was also apparent among some of the nurses interviewed. There may be several reasons why nurses are experiencing such dichotomy. Nurses have to deal with a plethora of regulatory compliance policies and could not conceivably abide by each of these policies to the letter, especially as a result of the at times unpredictable nature of the situations they have to deal with. As far as the nurse is concerned, saving a patient's life is their primary goal and if patient information has to be compromised in order to achieve the primary goal, then they have a choice to make. The reality is also that the nurse is human with a good sense of curiosity which may sometimes get her or him into the trouble of patient information breach. While not advocating for "excusable" breaches, one needs to be pragmatic and look at the whole situation before meting out heavy judgements against the nurse.

Some of the nurses mentioned that they did not feel they learned enough about patient information privacy in school. This feeling, expressed by nurses during the study has been echoed by Kamerer and McDermott (2020) when the authors mentioned that the common thread missing from previous informatics and health technology education has been the nurse's role in preventing and reporting cyber-threats and in maintaining cybersecurity. They go on to recommend that systems of higher education that educate healthcare and IT professionals should research and consider the feasibility and best practices of providing this education, as these workers are vital in helping to stop cyber-threats and security breaches in the field. The question would then be "how much is enough?" The nurse participants suggested that nurses be given a platform on which to voice privacy concerns. Although this request seems reasonable, the justifications for mounting such a platform could be quite complex, given the hurdles such as

legal implications and its administration that proponents may have to deal with. Nurses need to be made aware that they could call the practice consultant of their respective professional association CARNA or the SRNA. However, the alternative of defaulting to the public internet is worse. The interviewees clearly expressed that the avenues for learning patient information privacy were extensive and included nursing school, orientations, professional development, mandated training modules, fellow nurses, and reminders. Perhaps, instead of using such a broad avenue, some of which appear to be casual, evaluate the effectiveness of each of these avenues and select the most impactful for communication and education.

Perhaps, the general limitations in patient information privacy education is indicative of the limited availability of clinical informatics competencies in nursing to inform best practices in education. This informatics platform is often necessary for launching patient information privacy education. In a study that reviewed clinical informatics competencies in nursing to inform best practices in education and nurse faculty development, Foreman et al. (2020) found that, nursing educational programs do not adhere to standardized criteria for teaching nursing informatics competencies. This was corroborated by a literature gap in the scarcity of research related to informatics training requirements for nurse educators. There is a need for more education in digital health and informatics education (Nagel et al, 2020). Awareness is also needed for the CASN resources available (Nagel et al, 2020) and use of the competency requirements for RNs in Canada (CASN, 2012).

“Efforts to disseminate and integrate the digital health / informatics competencies into the undergraduate curricula of Canadian schools of nursing are ongoing” (Nagle et al., 2020, p. 1). Digital health, a term more commonly used in Canada (rather than informatics), refers to “the

use of information technology/electronic communication tools, services, and processes to deliver health care services or to facilitate better health” (Canada Health Infoway, n.d., as cited in Nagle et al., 2020, p. 2). Educators’ engagement and leadership support are vital for overcoming barriers and advancing informatics capacity in undergraduate education. Although there may be champions to lead the work of integration, all educators have a responsibility for teaching core digital-health related content and for contributing to informatics integration initiatives within their schools (Nagle et al., 2020, p. 13). The evolution of relevant future curriculum and course design will be contingent on the development of each educator’s competency in digital health/informatics (Nagle et al., 2020, p. 13). Educators need to be cognizant of the difference between digital health/informatics competency and basic computer proficiency and the fact that nursing students do not inherently have the former just because of their computer literacy. Further, educators need to be aware of the distinct difference between issues related to the use of digital health in clinical practice and the use of technology to deliver course content (Nagle et al., 2020, pp. 13–14). “Students should be encouraged to elevate and advance digital health discussions in classroom and clinical settings” (Nagle et al., 2020, p. 14). “Nurse administrators play an important role in supporting faculty in the acquisition, development, and dissemination of digital health knowledge” (Nagle et al., 2020, p. 14). “Increasing educators’ capacity in informatics is key for ensuring future generations of nurses are adequately prepared for competent and safe practice in digitally rich workplaces” (Nagle et al., 2020, p. 14) As stated by Risling (2017), “nurse educators, both in practice and education, will be essential in leading a successful technological evolution for nursing” (p. 91).

“In view of the current technological revolution impacting all sectors of society including health care, nurse educators are in a unique position to shape the future of nursing practice. Educator engagement and administrative leader support within every Canadian school of nursing are vital for overcoming barriers and advancing the informatics capacity of all future nurses” (Nagle et al., 2020, p. 2).

There were nurses who were concerned about the consistency of messaging with regards to privacy education between nursing units and indicated that the messaging should be tailored to inform new nurses and update existing nurses. Although this sounds simple, it may be difficult to implement due to the arduous task of first of all, defining “new” and secondly, tracking these “new” nurses through the nursing network. The confidence nurses have in privacy education was encouraging to hear in the interviews, and that, education will help curtail breaches. There is also the opportunity to explore non-conventional ways of education, such as nurses learning from other nurses and engaging nurses in the planning and development of educational course content.

6.5 Theme E: Nursing Practice

Nursing practice is a crucial part of who the nurse is, and goes far beyond the nurse’s jurisdiction. According to the Royal College of Nursing (RCN, 2020) in the United Kingdom, the principles of nursing practice describe what everyone, from nursing staff to patients, can expect from nursing. The RCN has enumerated some eight principles of practice that according to the organization, describe what constitutes safe and effective nursing care that cover aspects of behaviour, attitude, and approach that underpin good care. These principles include in a summary format, that nurses and nursing staff: treat everyone in their care with dignity and humility; take responsibility for the care they provide and answer for their own judgments and

actions; manage risk, are vigilant about risk, and help to keep everyone safe in the places they receive health care; provide and promote care that puts people at the center, involves patients, service users, their families and their care givers in decisions and helps them make informed choices about their treatment and care; are at the heart of the communication process - they assess, record and report on treatment and care, handle information sensitively and confidentially, deal with complaints effectively, and are conscientious in reporting the things they are concerned about; have up-to-date knowledge and skills and use these with intelligence, insight and understanding in line with the needs of each individual in their care; work closely with their own team and with other professionals; and finally lead by example, develop themselves and other staff to influence the way care is given in a manner that is open and responds to individual needs.

Most of the RCN (2020) principles directly or indirectly have implications for patient information privacy. One of the principles, “nurses and nursing are at the heart of the communication process...”, in particular, speaks to patient information privacy and provides the impetus for nurses to be responsible and accountable when it comes to patient information privacy.

There is another RCN (2020) principle that mentions the involvement of the patient’s family in care. This is another reason to take the issue of family member involvement seriously, as will be discussed subsequently. The RCN goes on to further suggest how the principles can be used to understand what patients, colleagues, families and care givers can expect from nursing, help nurses reflect on their practice and develop as professionals, and help patients and their

families evaluate the care they have received by using the principles as a checklist, which includes intentional protection of the patient's information.

The Canadian Nurses Association (CNA, 2015) has indicated that registered nurses practice across five domains including administration, clinical care, education, policy and research. The nurse's wide involvement in these five areas should indicate why nurses should have or exert significant influence in matters concerning patient information privacy. In their 2015 update to the "*Framework for the Practice of Registered Nurses in Canada*", the framework promotes advocacy, promotion of a safe environment, research, participation in shaping health policy and in patient and health systems management, and education. The CNA (2017), by way of their Code of Ethics has identified seven values that are important to nursing practice. In my opinion, at least four of these, namely; providing safe, compassionate, competent and ethical care; promoting and respecting informed decision-making; preserving dignity; maintaining privacy and confidentiality, and being accountable, relate to maintaining patient information privacy.

In discharging their duties, nurses face challenges. One of such challenges is having to deal with, or manage their own human nature, which if unchecked, could overcome a nurse's professionalism. The result may be infringement and violation of several patient information privacy policies. Analysis and discussion here would focus on dealing with the nurse's professional obligations and human nature, how the nurse deals with challenges and their consequences, privacy infrastructure, pressure from the patient's family, safe and unsafe practices, as well as trust and mistrust.

6.5.1 Sub-Theme: Professional Obligations vs. Human Nature

The nurse deals with a tremendous amount of information as part of her or his day-to-day activities that helps make informed decisions. Nurses understand that they need to access only information that pertain to the issue(s) they are confronted with. However, the set of information available to the nurse may have several components. The information could be “interesting”, “intense”, “scary”, “strange”, etc. These dimensions are often what get nurses in trouble by appealing to the human nature of the nurse. The nurses were also aware that the word “professional” was often associated with “trust”. Nurses believed that patients equated professionalism with trust. This meant that patients take it for granted that nurses will respect information confidentiality. Therefore, divulging information to the nurse, including personal information that has nothing to do with treatment, as mentioned before, was often without hesitation from the patient.

As indicated earlier, the nature of the nurse is defined in terms of their roles, beliefs, actions, likes and dislikes, character, feelings, and personality as they relate to patient information. The nurse was described as being dichotomously a protector and liberator of information, and a believer in the flexibility of information availability. According to the nurses, sometimes the natural tendencies such as a strong desire to seek information can be overpowering to the point that it could subdue the nurse’s professional obligation. Controlling such inordinate passion for information seeking and subsequently sharing such information would mean finding ways to keep those passions in check. This could be a challenging endeavor, and it is also important to note that admitting what appears to be a weakness should not be counted against the nurse but should be a first step towards finding a useful resolution.

Nurses clearly understood the privilege of having been chosen by the patient to share with them their very personal information. This privilege would often compel nurses to respect the privacy of the patient information entrusted to them. Exercising comportment and self-discipline do not come easily, but the nurses felt that their trust relationship with the patient was important and were willing to defy their natural inclinations in order to protect this relationship. This tendency to exercise restraint and discipline could be leveraged to harness privacy initiatives. One should not consider it unreasonable to assume that “do’s and don’ts” woven into the very nature of an individual are much easier to exercise and are likely to produce long-lasting results.

The nurses were also realistic about how a patient’s information should be handled. Throughout the data, the nurses described several scenarios of role reversal and were able to feel how the patients felt when their personal information was intentionally and/or carelessly divulged. The nurses were able to personalize the hurt, pain, disappointment, and other adverse effects. In many ways, nurses operated with the philosophy that they would do to others what they would have others do to them, as they have been patients before. In line with this thinking, the nurse was sometimes referred to as having a “dual individual perspective”, since the nurse used to give information as a patient, but is now receiving information. The commitment on the part of the nurse to keep the patient’s information confidential strengthened when the patient-nurse relationship developed into some kind of friendship. In such circumstances, some of the nurses were prepared to protect the patient’s information at all cost. One may be tempted to pass quick judgment against the nurse’s emotional attachment to a patient. While professionalism may call for detachment, the benefits of attachments should perhaps not be ignored but further investigated to establish how it could be used to strengthen patient information privacy. Evident

in the data was that nurses understood and took patient information protection as a serious responsibility. The Standard News (2020), has provided brief explanations of what in medical terms is referred to, as “the therapeutic nurse-patient relationship”, which according to the writer, is at the core of nursing practice. The five tenets of this relationship are trust, respect, professional intimacy, empathy, and power. It was apparent among the nurses who were interviewed that these attributes have become part of who they are. The nurses therefore, subconsciously spoke about the outcomes of the attributes rather than the attributes themselves. There was also the issue of the nurse's dislike for bureaucracy and in some instances, the nurses could justify the violation of rules. In situations where bureaucratic processes were perceived as hindrances to expedited solutions, some nurses did not have any problems putting the patient's needs first. An interesting observation during data collection was when a nurse told the patient that she/he was breaking the rules in the patient's best interest. This is probably to indicate the depth of the relationship between the nurse and the patient once the patient opened up to the nurse and was willing to share personal confidential information. As discussed earlier, this is a good indication of human nature that rules and regulations could hardly suppress. Subjective submission to privacy regulations by nurses is not what is being advocated here. Hard as it may be to admit, in many instances, reality would prevail. The big question is how to deal with such situations, and there are no simple answers. Some nurses appeared confused about the push for the patient's privacy and family-centered care as they did not think the two could co-exist.

6.5.2 Sub-Theme: Challenges vs. Consequences

According to the nurses, challenges they faced emanated from their practice environment, pressure from patient's family, and unusual situations including pressure from fellow nurses to

blatantly “break the rules” and fully access a patient’s identity. Such violations even extended beyond a nurse’s zone of influence, where a nurse could wander around and read information about patients not in their care. Although some nurses indicated their disapproval of such behaviours to the point of openly expressing their frustrations, it appeared that among the nurses, there were some sort of psychological contracts in which territorial work boundaries were not respected. This meant that some nurses were willing to lower their work boundaries and allow intrusion as long as this favour is reciprocated. Such “exchange transactions” among nurses were often not planned but happened and were tolerated by some nurses. Dealing with such permissiveness may require further investigation and education. The nurses also pointed out that the user unfriendliness of their user interface was sometimes a challenge. There were no indications that this challenge has been reported to the administrators. If there is no forum for expressing such frustrations, as the nurses put it, the tendency is for the nurses to find their own workable solutions that may not necessarily be in compliance with privacy mandates. The notion by the nurses that parts of the patient information privacy regulations were restricting was also a concern by the nurses. The nurses believed that their primary goal and focus was the well-being of the patient. Thus, any mandates that do not foster this goal and focus but impedes progress in any way is likely to be perceived as roadblocks. As some nurses implied, if they have to break the rules to save a life, they would rather save a life

6.5.2.1 Privacy Infrastructure. Placement of their nursing stations was another challenge for the nurses. On a number of occasions, the stations were placed in public view, particularly, nursing stations on wheels. Nurses reiterated the need to be cautious especially with electronic records as extensive amounts of the patients’ information could be accessed with a few

mouse clicks. Some nurses had learned to rely on the computer security system to protect access to patient information, such as self-shutdown by the system after a certain period of dormancy.

While this feature may be prevalent on many systems, its appropriate use by nurses may be questionable. Protection afforded by such a system is user dependent. User training in its use is therefore important not only for self-shutdown but the many other security features built into the nursing station. The issue of discussing patients' personal information in public places was raised as a concern. It may be "easier said than done" when it comes to situations of this nature. A nurse may have a pressing need that may have to be dealt with sooner than later, and may be overwhelming as well. In many of such situations, the human nature is likely to take over. Rationalizing and careful thinking may be replaced by chaos and emotions. There are no simple answers here. Nursing administrators need to be aware that such situations exist and provide appropriate support to nurses. A nurse suggested that there may be the need for what the nurse termed "privacy for reflection" for the nurse. This meant conscious seclusion to deal with overwhelming patient issues rather than spontaneous unconscious sharing regardless of location. The infrastructure to accommodate such important occurrences may not be available in a healthcare facility.

6.5.2.2 Pressure from Patient's Family. There were several challenges the nurses were faced with, when it came to patient information privacy and the patient's family. The term "family" as used here connotes direct family members and other close or significant relations. Such challenges included pressure from family members to release patient information and the fury nurses had to deal with when they were unable to do so. The feelings between the family members and the nurse sometimes got so intense that a nurse suggested that dealing with the

patient's family was the worst among all the challenges nurses faced with regards to patient information privacy. Family members would often be frustrated as the nurse followed the existing protocol regarding divulging of patient information and the family members expected the nurse to have all the answers. Directing the family members to a more appropriate avenue for requested information often did not sit well with family members.

On occasions, dealing with the media and the police demanding to talk to certain patients in addition to the demands from the patient's family made the nurse's life even more difficult. Although the nurse is multi-talented and able to deal with various situations, demands of the nature described above takes away the nurse's attention from pressing medical issues. Sometimes it may stand to reason that certain responsibilities such as dealing with the patient's family, the public and other agencies be off-loaded to allow the nurse to focus on providing medical attention to the patient. Asking the family members to step out during rounds was another difficult thing for nurses to do, as some family members did not take this well. This "unwelcomed" request by nurses sometimes put further strain on the nurse-patient family member relationship. Nurses often have to work with the patient's family members in the best interest of the patient, such as in situations where the patients cannot speak for themselves and the help of the family member is needed. Education of nurses in patient family member relationship could go a long way to enable a better understanding between these two parties.

6.5.2.3 Consequences. Nurses suggested through their responses during the interviews that the harsh realities of the consequences of patient information breach are still latent. A point also apparent was that ignorance of these consequences has almost become the norm. Perhaps, part of the reason for lack of "fist-waving" in the nurse's work environment is to create a work

environment that is safe and non-threatening. After all, who would like to be threatened with a job that they have dedicated their lives to? If the intention of alerting nurses to the consequences of breaches is to use fear of termination or loss of license as a deterrent, it may not produce the desired results. The nurse's work environment may have conditioned him or her not to fear.

Using guiding principles that appeal to the nurse's conscience and emotions may be better alternatives to fear mongering. There was the suggestion from a nurse that sometimes, letting patients share how information breach has affected their personal lives can be very powerful.

6.5.2.4 Safe v. Unsafe Practices. As indicated under the presentation of results, privacy of information is also taken to mean "safety" of information from outside parties. Privacy could be described in many different ways to conjure the illusion of absolute protection. Important to note was that relentless efforts to protect patient information should not translate to promise or guarantee of certain privacy. As a nurse insinuated, in a perfect world, the ideal would be the norm but our world is far from that. The nurse also remarked that the expectations of the professional bodies are often unrealistic. While the nurse's remark may not be one to be readily dismissed, the virtue in expecting high standards from nurses should not be frowned upon either.

The big question is, where does one draw the line when it comes to protecting patients' information privacy? What should the threshold be, even if lowering the privacy standards was a plausible and practical proposition? There are no easy answers. On occasions, the nurse would actively monitor the patient's environment regarding who was coming in and leaving, and engage the patients in managing their information and privacy.

6.5.2.4.1 Nurse's Discretion. The use of the nurse's discretion in managing the safety of the patient's information was mentioned. For example, dealing with phone calls that came in for

a patient was at times left to the nurse's gut instinct or judgement call. This approach to handling the management of a patient's information would seem practical given the unpredictable nature of requests coming from the nurse's domain. Prescribed responses to such requests are not feasible. Allowing the nurse to exercise discretion should go a long way to reinforce the trust and confidence the nursing managers have in particularly, the front-line nurses. The freedom for the nurse to exercise personal judgement, coupled with directed (use of personal experiences) training should serve the use of discretion well.

6.5.2.4.2 Audits. Concrete ways of ensuring patient information safety, according to the nurses, included the use of audits to monitor access to patient information. This is an electronic audit in which every move and use of the nursing system by a logged-in nurse including mouse clicks may be tracked and recorded. The hard reality is that the logged-in nurse often has no idea that he or she is being tracked by the operating system. At times, systems administrators turn on system auditing to ensure nonrepudiation. Clearly, the point should be made that auditing is usually not an attempt to make victims or "witch hunt" for system misuse. Auditing is a tool for system administrators to ensure accountability and gather information for troubleshooting when there is a problem. Some nurses believe that paper records are more secure.

6.5.2.4.3 Electronic v. Paper Records. There is another group of nurses who think electronic records are more secure. From what nurses said in the interviews, the contention was about the degree of perceived safety of these two different ways of keeping the patient's records. Proponents of better protection with paper records suggested that the process of physically accessing a patient's records could be laborious and difficult, and this difficulty in itself constituted a barrier to ready access to records. Nurses that believed in the superior protection

offered by electronic record keeping pointed to the ease of ensuring information safety. Requiring login information and the capability to track logged-in individuals made electronic record keeping attractive.

6.5.2.4.4 Effectiveness and Efficiency. A great deal of resources could be used in ascertaining the merits and demerits of both paper and electronic records purely from the information protection perspective. The reality, however, is that other measures of performance such as effectiveness and efficiency may be important parameters that could take precedence over information protection for the purpose of privacy, in the nurse's work environment.

Williams et al. (2018) have defined efficiency as getting work done with minimal effort, expense or waste. The same authors say that effectiveness means accomplishing tasks that help fulfil organizational objectives such as customer service and satisfaction. Given the working meanings of these performance measures and their relevance to budgetary constraints and the primary goals of the nurses, it is not difficult to understand why a nurse would choose efficiency and/or effectiveness over information protection.

6.5.2.4.5 Duplicate Patient Information. Regarding patient information safety, a nurse mentioned the use of duplicate patient information, one paper, and the other, electronic. The nurse indicated that as a result of home visits and the possibility of losing patient records, the different formats afforded the nurses some safety. While the duplicate and different formats the nurse's unit employed took care of continued access to patient information, the lost information could be in the hands of someone. Efforts at protecting the patient's information suggested by the participants of the research included hiring a very good network administrator. The network administrator is key to ensuring the security of the patient's information. However, this person is

only one of the many factors that work together to ensure safety. According to a nurse, patient information safety was a discipline drilled into them as part of their nursing training and also part of continuing education.

6.5.2.4.6 Education/Patient Information Privacy. Education in the need for patient information privacy would likely produce a lasting effect. Nurses are likely to learn core concepts in privacy and the underlying reasons for why breaches occur. This deeper understanding as a result of education would likely lead to better attitudes and preventive measures coming voluntarily from the nurses. Rationalizing the need for patient information privacy would appear to be more appealing to nurses than forcing them to comply with mandates and stipulations.

6.5.2.5 Trust v. Mistrust. This issue of trust and mistrust between nurses and patients could be an interesting one. The assumption can be made that patients willfully divulge personal information to nurses as a result of a trust relationship between the nurse and the patient. What is true, as a nurse put it, is that nurses continue to take the issue of confidentiality seriously if they are to be trusted. When it comes to providing information whether for treatment or identification, patients often have no choice. What is fairly easy to assume is that patients provide information primarily to receive treatment and hope that this information is protected. Trust is built over time and as another nurse said, it comes with responsibility. Of interest, as responses to the interview questions revealed was that a nurse entertained the thought of the possibility of punishment for breaking trust as a result of behind the scenes monitoring. The fear of being watched, discovered and eventually punished would become a deterrent to inappropriate behavior. Although this would contribute towards minimizing privacy violations, the absence of punishment or the fear

of it would result in reverting efforts made towards privacy compliance. In some instances, nurses personalized the assumed trust of the patients and felt personally chosen to share in the patient's life. There appeared to be some level of emotional involvement by the nurse that conjured commitment to uphold and respect the patient's privacy. Important questions researchers may want to seek answers to are, what prompted this reaction, and whether the level of commitment could be replicated. The reason this may be an act to follow is that decisions that are made not only cognitively but also from the core of an individual could become that person's second nature.

6.6 Theme F: Electronic Records and/or Paper Records

There are several diverse perspectives between nurses when it comes to choosing between electronic patient records versus paper records. Often, the responses nurses provided depended on the nurses' work experience and years of services. There were nurses who believed that the technological advances brought on by electronic record keeping has greatly facilitated expedited patient information exchange and ultimately helped save lives and ease management of patient records. There are several virtues and shortfalls with electronic and paper records. These virtues and shortfalls often make it difficult for nurses to agree on which one should be preferred over the other. The next few paragraphs highlight and discuss some of the findings during data collection and analysis.

6.6.1 Secure v. Vulnerable

There was the general thinking that electronic records were more secure than paper records. The thinking was that paper records are readily available whereas electronic records

have many safeguards such as pop-up warnings, difficult to access due to the knowledge of the system required to gain access, which in itself is a barrier, the multi-layered permission system, the ability to track, monitor, and audit users of the system, and the many other security features of the electronic system. Nurses who believed that paper records are more secure based their reasoning on the physical nature of paper records. For example, it is easy to see a nurse who does not have permission fiddling with patient records. While electronic records could be accessed remotely, physical access is required with access to paper records. What was also rightfully pointed out was that paper records are not susceptible to hacking. Bulk access by hackers of electronic records could be a real possibility, while the same level of access to paper records by intruders can be challenging.

Weaknesses with paper records that were mentioned by the nurses interviewed included readily visible stickers on patient files. These stickers often have patient identification information, etc. Nurses were a little worried about mislabeling the files and the possibility of misdiagnosis. Although this is beyond the scope of information security, it was disturbing enough for the nurses to bring it up. Another vulnerability of paper records that came up was the easy misplacement of paper records. A nurse narrated an incident that is uncommon. The nurse talked about how a patient seized paper records and would not return them. Misfiling of paper records was also a concern. One vulnerability that nurses who believed in paper records mentioned was when nurses vacated their electronic stations without logging out, the entire system was left open. Sometimes, such vacations have been unintentional and have occurred for example, as nurses responded to emergencies.

Health regions appeared to be at different stages of transition from paper record to electronic record keeping. The use of paper records appeared to be pervasive in the Saskatchewan health region. Electronic record keeping is prevalent in the AB Health Regions. Evident during the interviews was that both regions used some sort of a hybrid system. Nurses in the AB Health Regions indicated their preference for electronic records and made several positive comments regarding electronic records.

6.6.2 Benefits v. Pitfalls of Electronic Records

The nurses believed that electronic records cut down on paper floating around, electronic records could self-protect using techniques such as screen shut down when left idle for a certain period of time. Electronic records can follow a trail of activities. The ability to easily capture and transfer electronic records securely to facilitate information exchange and sharing was also a benefit the nurses mentioned. Speed of access to electronic records contributing to efficiencies, ease of use, and bulk access to patient information were enumerated as gains for using electronic records. The nurses also appreciated the fact that electronic records curtailed asking the patient the same questions by different people, fostered portability, and minimized transportation of paper records leading to reduced record contamination. Some described electronic records as that which provided “one-stop-shop” for almost all patient information, and on another occasion making “electronic” synonymous with “availability at all times”. According to a nurse, electronic records compensate for poor doctor handwriting. Another nurse spoke from the patient’s point of view indicating that electronic records made the patient’s information available to medical specialists for the most part, regardless of their location.

Nurses' perceived shortfalls of electronic records included the ease with which electronic records could be easily copied or deleted remotely. The nurses mentioned that sometimes printed materials ended up with the wrong printer, revealing otherwise confidential information to an unintended recipient. The different electronic record systems made it difficult to share between systems as a result of incompatibilities. For the nurses who struggle with the electronic age, the electronic record system could be a real challenge. Some nurses considered the user interface of the electronic record system non-user-friendly. There were others who appeared to be complaining about the change from paper to electronic record keeping. Their concern was the learning curve associated with the change. A nurse commented that getting used to paper record keeping to the point of knowing where everything was and changing to learn a new system was a "chore". Electronic records also made it easy for prying eyes. The nurses indicated that a lot of damage could be caused by only a few clicks of a button.

6.6.3 Benefits v. Pitfalls of Paper Records

A participant commented that paper records made the nurse feel that she or he was working. Some nurses also commented that physical presence of a patient's file afforded the nurse some level of control over the privacy of the patient's information.

Nurse participants said that they had difficulty identifying snoopers when it came to paper records. Easy access to rooms with paper records was another problem. Participants added that outsiders using social engineering, dressed appropriately like nurses could gain easy access to the nursing floor, and charts. On this note, some of the nurses voiced their frustrations at doctors who strayed in with street clothes. The nurses indicated that sometimes the volume of records a nurse may have to handle could be overwhelming, especially if the patient has been in

and out of the medical system several times. According to the nurses, the time spent waiting for retrieval of such records could be frustrating.

6.7 Theme G: AB and SK Health Regions

The AB and SK health regions currently are both actively involved in the pursuit of electronic record keeping. However, the two regions appear to be in different places when it comes to electronic record use. During the study, participants in the AB health region appeared to be better informed when it came to electronic record use. Historically, mention of AB-initiated electronic health record has been as early as 1988 at Foothills Medical Centre in Calgary (Walker et al., 1988), so AB was not only earlier than SK but far ahead of most American cities of the same size or larger. In the booming economy of the 1980-1990s in AB, the province possessed the infrastructure and resources needed to advance with the new technologies, while SK at the same time was a “have not” province in terms of economy. SK, a province of only a million people did not initiate electronic records until well into the next century, when their economy much improved. This section briefly discusses some similarities and differences in the two health regions, as well as a quick look at resource availability with regard to patient information.

6.7.1 Similarities vs. Differences in AB and SK

Throughout the study, it was clear that the hybrid system of patient information record system was pervasive in both AB and SK Health Regions. Each of these regions may have a different mix of paper and electronic records. There was a high likelihood of finding more electronic records versus paper records in the AB Health Region than one would find in the SK health regions. There was the general feeling among the SK participants that electronic record

keeping was recent. A participant indicated that it was apparent the Saskatchewan Health Region was behind when it came to electronic record use.

6.7.1.1 Resources v. Limited Resources. Nurses in AB appeared to have access to several resources with regards to ready access to patient information. A participant commended the rigour of the Alberta patient information privacy and security resources. Some participants in the Saskatoon Health Region thought that healthcare in the region was being ignored and that patient information breaches by nurses were intentionally done to get attention. While this feeling expressed by a respondent was not pervasive, it may be prudent for the administrators to look for other signs that corroborate this nurse's assertion.

This chapter 6 has provided a discussion about what was captured from the nurses regarding their thoughts, feelings, perceptions, etc. using a thematic approach. The nurses have clearly demonstrated that patient information protection is of significance to them. They have also provided hints on some categorical areas in breaches that need attention. The discussions shed light on what the nurses did or did not do and the implications of the findings for the nurses' personal lives, nursing practice, policies, and other related areas. I have also shared my opinions on the observations made. The latter part of the discussion looked at the benefits and pitfall of electronic and paper records. It was clear that AB was well ahead of SK in the use of electronic records. In terms of the attitudes, perceptions, etc. towards patient information privacy, not much difference was noticed.

My personal reflections, coupled with the moderate journal I kept for the study often "took" me to several places mentally. Having seen nurses at work in different places, situations, and circumstances, the biggest question I have always asked myself is, how are nurses able to

cope with the myriad of responsibilities including following patient information privacy mandates and keep a smile on the face, reserved for their patients? When I have posed this question to nurses, the answer has often been blithely “because we are special”. The little interactions I had with nurses during the study make me believe in all sincerity that nurses are indeed special people. I am sometimes inclined to think it is a learned behavior, perfected over time.

When I made the decision to pursue the study of nurses’ experiences in patient information privacy, part of me questioned how I was going to be received by the nursing community given that I am not a nurse, and far from being one. The other part of me was thinking that I may be a good candidate particularly because of the subject matter, privacy of patient information. The thinking I had was that nurses may be uncomfortable sharing with their fellow nurse some unpleasant experiences or what they may perceive as embarrassing moments. I would hasten to say that I was very well received. One surprise I would like to mention is the openness on the part of the nurses and their willingness to share some intimate experiences. I must mention that I met and interviewed the nurses outside the hospital or clinic environments. I have also always wondered how different the outcome would have been if they were surveyed in a hospital or clinic environment. The research subjects remained calm and relatable throughout the interview process. Majority of the nurses I interviewed had been nurses in several different places and thus were able to provide perspective. It was also interesting to learn that privacy was personally important to the interviewees. A number of the nurses indicated that change and the frequency of it in patient information privacy policies was something they had to learn to cope with, but still not used to.

Something else I learnt that was interesting in my opinion was when the older nurses said they took it upon themselves to provide the younger nurses some orientation in patient information privacy. In retrospect, I wondered what the response would have been if I had questioned the older nurses about what prompted this initiative. Perhaps, what surprised me was the added responsibility the older nurses took to consciously and repeatedly remind the younger ones. The role of gender, age, ethnicity as demographic data will be interesting for further research. A few of the nurses indicated that AB appears to have what they described as “too many information systems that often will not talk to each other”. This was with reference to electronic record keeping. Other things some of the nurses brought up was why nurses are often the victims of patient information breaches, and not doctors. I also noticed that a few nurses would just answer the interview questions and not be chatty about the subject, particularly in the Saskatchewan region. One big surprise to me regarding electronic systems was when an interviewee mentioned that their electronic systems included nurses texting physicians for orders. My surprise simply stems from texting and patient information protection. The idea that paper records were more secure than electronic records was espoused by older nurses.

CHAPTER VII – RECOMMENDATIONS, LIMITATIONS, FUTURE RESEARCH OR IMPLICATIONS FOR PRACTICE AND CONCLUSION

7.1 Recommendations and Implications for Practice

In order to put the recommendations that are presented in this section in perspective, it is important to revisit the fundamental under-pinning of this research. The purpose of this research was to gain a better understanding of the experiences of registered nurses in patient information privacy and security in the AB and SK health regions. As indicated under the “Research question” section of this thesis, specific goals of the study included capturing rich insights to perceptions, feelings, reflections, thoughts, apprehension, and comprehension in relation to patient information privacy and security as the nurses go about their day-to-day activities. The hope was that such insights would lead to understanding what is important or not important to nurses, ascertain specific implications, provide clues to understanding some existing behaviour patterns, and to inform future research. Also important to mention was that the research was exploratory in nature.

The primary research question was broadly stated as “what are the experiences of medical-surgical/critical care registered nurses as they comply with health information acts”. Other relevant questions related to the primary research question are “what meanings do nurses bring to patient information privacy and security practices?”, “are nurses concerned about the expectations mandated by health information acts?”. As defined earlier, “experience” in the context of the proposed study is: “the actual living through an event... the real life as contrasted with the ideal or imaginary ... The sum total of the conscious events which compose an individual life” (Erlich, 2008, p. 1126). This research study provided the opportunity to delve

into the experiences of RNs in patient information privacy and security to discover what they have observed, encountered, or undergone in the course of time. This chapter focuses on recommendations that emanate from this research work including problems or issues that came up as a result of the research, including what may be termed “discoveries” that may require further probing by way of future research. The recommendations have been categorized into academic (further research), policy makers decisions, practitioners, education and training.

7.1.1 Academic

- The study looked at the nurses’ experiences as a whole and did not partition these experiences by the nurses’ years of service experience. A future study to investigate by age groups and do a comparative analysis of the different age group experiences would be interesting.
- When it came to attitudes towards breach by the nurses, there were mixed feelings among nurses. There were even those that believed that sharing is the second nature of the nurse, with others believing that breaches will never stop. Many nurse participants thought that a key reason for breaches was curiosity (seeking interesting information). Others reiterated that information of famous individuals will always be breached. Through further research, it would be interesting to delve a little deeper into what nurses are really thinking.
- When it came to the issue of electronic records versus paper records with regard to patient information privacy, the nurses appeared to have split opinions. Although the tendency is for most healthcare regions to move towards electronic record keeping,

hybrid record keeping is also common. Research work comparing electronic and paper record security could help expedite the transition or assist in decision making when it came to these two record types.

- During data collection, it was pointed out that the commitment on the part of the nurse to keep the patient's information confidential strengthened when the patient-nurse relationship developed into some kind of friendship, making the nurse even more determined to protect the patient's information at all cost. Further research to gain a better understanding of this relationship and the subsequent commitment to protect the patient's information may be worthwhile.
- An area in the nurse's work environment that may be interesting to investigate further by way of research is what a nurse called family-centered approach to nursing and patient information privacy. This area may be particularly important as the nurses had significant difficulty managing it.
- Another area that was interesting to hear about but may be a little difficult to investigate is what I labeled earlier in a section as “psychological contract” between the nurses, which allowed a nurse to traverse into another nurse's work territory in search of information, a favour that may have to be reciprocated. This was some kind of exchange transaction that could be described as insidious.

7.1.2 Nursing Administration Policy Makers' Decisions

- The study may have implications for policy decision making. Some of the participants indicated how they feel and think about some of the policies they have to comply with.

Such claims by the study participants could be further validated and possibly provide avenues for significant bottom-up approach to the formulation and implementation of privacy and security policies and guidelines. The reason for this suggestion is simply that policies and guidelines informed by its participants, especially, the “frontline actors” are likely to be well received and have a better chance of achieving what they were designed to do.

- There may be the need to establish a peer-to-peer forum for practicing nurses to hear and/or share experiences regarding patient information privacy and provision of channels for escalation to decision-makers. This may reduce the coffee room discussions and other activities that compromised or often led to patient information breaches, as was evident in the study.
- The findings of the study may provide policy and decision makers a better understanding of the complex (dynamic) work environment of the practicing nurse that could help moderate the expectations for the nurse. As noted in the literature by Cornell et al. (2010), the chaotic pace of the nurse’s environment implies that the nurses rarely completed an activity before switching to another.
- The nurses were unclear what monitoring policies were in place regarding patient information privacy. The personal concerns that the nurses had included what some referred to as careless abandonment of open workstations as the nurse “veered” to grab a cup of coffee, common sharing practices such as the use of faxes, emails, etc. even for sharing patient information. The nurses also indicated that there did not appear to be

consequences for logging into generic workstations and not logging out. This situation could be further investigated and corrective actions taken if necessary.

- Some of the nurses who were part of the study used hard language when it came to talking about breaches. These nurses mentioned that breaches could be as a result of the lack of morality on the part of the nurse, due to malicious intent to draw attention to an issue, portray emotional feelings and to bring about change. Patient information privacy policies, regulations, and guidelines may have to clarify that the above infringements constitute violation that could carry serious consequences. Some participants suggested that breach is not taken seriously by the nursing community.

7.1.3 Support for Educational and Practice Training Resources

- In a number of situations, what changing of behaviour calls for may be a change in attitude. The nurses did indicate that being intentional about “respecting” the patient’s privacy could provide the desired results. This should not be taken as an ultimate solution to patient information privacy. This claim by the nurses may need to be validated possibly empirically. Education and training initiatives that target “attitude adjustment” could lead to deeper and lasting change. This also means that education and training models aimed at mechanizing and forcing participants to abide by set rules may only produce temporary solutions.
- The nurses mentioned a number of attributes that could help guide training of the nurse in the area of patient information privacy. The nurses encouraged the need to follow the rules as a matter of ethical duty; for the nurse, privacy is a matter of due diligence; privacy has to do with “need to know”; privacy could entail divulging a level of patient

information but leaving out details; privacy initiatives should consider data transmission, proximity of others. The above are some of the utterances from the participants. What the nurses said could be used to possibly guide training programs.

- There was the indication by the nurses that regulatory compliance was not a problem, but interpretation sometimes was. Other times, the language the regulations were written in, was a concern. Again, this claim could be confirmed through quantitative study. Policy or regulation administrators may then put together education and training programs that address the concerns mentioned above.

- There were a number of breaches that were classified by the participants as unintentional. In the eyes of the regulation enforcers, unintentional breaches may just be excuses. Nurses should clearly know what constitutes a breach. Breaching incidents could be used in education/training the nurses. However, the reality could also be that the nurses have problems distinguishing between what constitutes a breach and what is not a breach. This means that administrators should proactively find avenues to inform nurses about breaches and not make it a mystery. There were nurses who explicitly mentioned that breaches were occurring as a result of lack of education. This assertion may need further investigation before putting together meaningful educational or training programs.

- A number of the interviewees mentioned that some nurses did not take patient information protection seriously as the consequences of breaches were often mild and not punitive enough. Administrators should be educated on the recognition of the early signs of breach occurrences and mechanisms for dealing with such issues before they become pervasive. Although the consequences of patient information breaches have been well

documented and categorized, the administrators may need some training in the appropriate meting of such consequences in order to produce the desired results.

- The issue of nurses not fully comprehending some guidelines, regulations, and rules as a result of the legal undertones was also a concern. It is recommended that nursing administrators are first of all, educated on such matters so they can explicitly address such issues by forming temporary teams of nurses and legal practitioners to discuss and learn from each other the most appropriate approaches to documenting such regulation, guidelines and policies, etc. Also, the one-page “InfoLaw” handouts published by Canadian Nurses Protection Society (CNPS) can be excellent materials to incorporate in education and training sessions. Efforts should be made to intentionally bring attention to such useful material that enhance the nurses’ understanding of the laws, regulation, policies, etc. for the nurses. One example is confidentiality and privacy (CNPS, 2020).
- Although tougher repercussions for violating privacy rules have been suggested above, a balance between self-reporting errors and punishments should be maintained and is likely to require a great deal of administrative education and training. Rodziewicz et al. (2020) have shared some thoughts on self-reporting of medical errors that have implications for patient information privacy errors. The authors suggested working towards maintaining a culture that works towards recognizing safety challenges and implementing viable solutions rather than harbouring a culture of blame, shame, and punishment. They go on to suggest that healthcare organizations need to establish a culture of safety that focuses on system improvement by viewing medical errors as challenges that must be overcome.

The suggestions made here for medical errors will work well for patient information privacy errors by nurses.

7.1.4 Practitioners

- Frontline workers may appear to be passive or not actively involved, and totally dependent on others, such as senior administrators, policy makers, etc. Nurses are very well educated and do have significant discretion. Nurses can work on improving communication among themselves and administrators. For example, there was mention of the user unfriendliness of the user interface being a challenge by some nurses but there were indications that this has not been brought to the attention of administrators. The nurses themselves could take the initiative to promote such communication among themselves and their managers. As the nurses put it, if there is no formalized forum to express such frustrations, the tendency is for nurses to find their own workable solutions that may be violation of privacy mandates.
- There was what appeared to be petition by the nurses to off-load certain responsibilities from the nurse to allow them to invest their time in better patient care. For example, the nurses were sometimes overwhelmed with what a nurse referred to as the worse issue they have to deal with, working with patient families.

7.2 Limitations

Although this study was exploratory in nature, it would have been interesting to dig a little deeper into certain areas such as some of the areas that the nurses thought were problematic in maintaining patient information privacy, such as the relationship between the nurses and the

patient's family through progressive elaboration. Previous research in this area is quite limited, and thus a significant gap. As a result, there were limited experiences to draw on.

Due to the sensitive nature of the subject of patient information privacy and security, at times, it felt as if some of the nurse participants were exercising caution or reservation with their responses. As a result, sometimes their responses were not as "raw" as could be, in my estimation. This same sensitivity at times made it difficult to recruit participants.

The research set out to investigate the nurse's experiences in patient information privacy and security. As the study progressed, "security" was subsumed by the meaning of privacy. In the end, the participants made "privacy" and "security" assume the same meaning. The logic would be that, we secure to ensure privacy.

Although qualitative study like this one affords several benefits including a first hand experience of the feelings and thoughts of the study subjects, generalization of the findings should be done with caution.

It is also important to mention that nurses in the category 18–30 years were few in number due to the snowballing recruitment used during the data collection (nurses already participating suggested or recruited their colleagues of the same age). This is an interesting age group, particularly when it comes to electronic records and social media use. Although their direct perspective is not presented here, some of their defining characteristics regarding patient information privacy experiences can be gleaned from the age group immediately after them.

7.3. Summary of Findings (Implications for Practice)

In order to provide a brief discussion of the implications of the study findings, it may be necessary to provide a recap of the findings. The study, as outlined earlier captured two umbrella

themes. One pertained to patient information availability and efforts to protect this information.

The other had to do with what nurses did or did not do that resulted in the breach of patient information protected by acts and statutes. Each of these two main areas (themes) consisted of component parts that crystallized into the themes from which lessons could be learned (the components and their parts), form the basis for policy formulation and reforms, confirm what has been previously discovered, and lead to further research. Each of the two themes were the subjects of the following subthemes under which the nurses consciously or subconsciously elected to narrate their experiences. The themes or subthemes included the following areas:

- Access to patient information (open or accessible versus restricted access, too much versus too little information, sharing versus protecting of information).
- Education of patient information (awareness versus ignorance, knowledge versus insufficient knowledge, education versus lack of education).
- Nursing practice (professional obligations versus human nature, challenges versus consequences, safe versus unsafe practices, trust versus mistrust).
- Electronic records and/or paper records (secure versus vulnerable, benefits versus pitfalls).
- AB and SK health regions (similarities versus differences in AB and SK, urban versus rural, resources versus limited resources).
- Similarities and differences between nurses in the two provinces, AB versus SK.

The nurses conveyed their perceptions, feelings, thoughts, reflections, ideas, suggestion, comprehension, and even apprehensions in the areas listed above, and often, without reservations. What the nurses had to say regarding the list above have the following implications:

- Appraising continually, selected nursing practices or behaviours in patient information privacy and security. For example, taking a closer look at some sharing practices such as emails and electronic transfers in general.
- Training and education of patient information protection not only consider direct technical skills but the person of a nurse as a whole, and his or her extended responsibility such as being aware of a nurse's custodian role as well as professional obligations when it comes to patient information.
- Ensuring that all nurses have the same interpretations or understanding of regulatory compliance relating to patient information privacy.
- Exercising a greater level of vigilance among nursing administrators, knowing that some breaches can be intentional.
- Monitoring social media websites to see the possibility of misdirected complaint's by nurses manifesting as venting episodes.
- Revisiting and reforming the consequences for patient information breach to make them impactful.
- Dealing with curiosity. While curiosity may be a virtue for professions such as nursing, the study participants indicated quite overwhelmingly that curiosity can be a double-

edged sword. Most breaches that occurred among nurses could be attributed to curiosity.

There needs to be deliberate efforts to deal with this issue.

- Defining clearly what amount of information from the patient is considered sufficient, and defining sufficiency in the appropriate context.
- Developing creative ideas by nursing administrators to ensure that breaches are taken seriously.

According to Leino-Kilpi et al. (2001), it is the duty of the registered nurse to report any malpractice witnessed or violation of patient right. Such reporting was rare in the study, although there were mentions of blatant violations in some instances during the study. Moore (1997) suggested that from the point of view of ethical theory, privacy is a curious value. He went on to say that privacy seems to be a matter of individual preference, culturally relative, and difficult to justify in general. The nurses that were surveyed voiced what their preferences were, with some indicating their misgivings about privacy when it came to nursing practice. The thinking espoused by Nissenbaum (2010) that privacy is not an absolute value but a form of contextual integrity was supported by study participants, with some going as far as indicating that “breaches will never stop”. Parks et al. (2011) agree as suggested under the recommendations section that mitigating identified privacy threats takes education and training. They added another human dimension, building a culture of privacy. Privacy impact assessment has also been suggested by the same authors. As the nurses confirmed during the study, there is significant trust between the nurses and patients when it came to the security and safety of patient information. This is an extension of research findings by the Canadian Infowaysurvey in 2007 (CI, 2007). Complaints by the study subjects regarding unintended exposure of patient information on monitors are not

isolated and new incidents. A study conducted by Stone et al. (2005) in England reported the visibility of information on computer screens and the difficulty of maintaining confidentiality in a busy waiting room. The reality of this problem means that something has to be done and not continue to be ignored. The autonomy for nurses as advocated by Weston (2010) in decision making, including the ability to act on one's own knowledge and judgment, taking into consideration the framework for pertinent laws, rules, organizational policies and procedures was not obvious in the outcomes of the study. Autonomy in decision making was at best, cursory in nature and did not appear to be organized. Benner (1984) has suggested that there is a wealth of untapped expert knowledge embedded in the practices and knowhow of expert nurses that remains unrealized unless it can be articulated by nurses.

7.4 Conclusion

The goal and objectives of the research study, as were stated earlier could be summarized as gaining better understanding of the nurse's experiences in patient information privacy. Such experiences would often show as the nurse's perceptions, feelings, reflections, thoughts, ideas, suggestion, comprehension, and even apprehensions. These attributes often showed up as verbal expressions captured during the study. The researcher, together with the research participants have thus, co-constructed a thematic portrait of the concerns, understanding, beliefs, cognitions, and interpretations nurses bring to patient information privacy and security. This section thus broadly describes important aspects of the research findings, highlighting responses to the research question(s), and how the aims and objectives of the research study have been achieved. The significance and implications of the study's relevant findings, as well as the contribution(s)

the research study findings have been summarized in Section 7.3. It is hoped that healthcare policy makers, researchers, and nursing professionals, who are the primary stakeholders of patient information privacy and security would make use of the findings.

The knowledge and experiences shared by the nurses during this study go to confirm what has been known for a while, the repository of knowledge within the nursing community. This wealth of knowledge and experiences were captured under themes and subthemes presented earlier.

7.4.1 Key Definitions Interpreted/Co-Constructed from the Data

While attempting to answer the primary research question of what the experiences of nurses are in the area of patient information privacy, there were lingering questions such as “what meanings do nurses bring to patient information privacy and security practice”. The following throws some light on the meanings and what was learned, as gleaned from the study.

Patient Information Security/Privacy. There is a relationship between nurses and patients with regard to patient information safety/security. Patient information safety/security involves a significant trust between nurses and patients of patient information. Nurses secure to ensure privacy.

Patient Information Security. The meaning of patient information safety and security was often subsumed by the definition of privacy. This therefore meant that the terms “privacy” and “security” were used interchangeably by the nurses.

Patient Information Privacy. Although the CARNA (2014) defined privacy as the general right of the individual to be left alone, to be free from interference, from surveillance,

from intrusion, and from interruption, the nurse-patient relationship could redefine information privacy.

Patient Information Breach. A breach of patient information depends on the set of rules or regulations mandated for access, retention, and dissemination of patient information. A breach is said to occur if these mandates are violated. These breaches were described by the nurses as intentional or unintentional. There was also the suggestion that some nurses did not have a clear understanding of what constituted a breach. There were indications that the nurses were not clear what the consequences of breaches were, with some suggesting that the consequences they were aware of, did not go far enough to be deterrents. A few respondents boldly articulated how they do not think that breaches are taken seriously by the nursing community and went further to suggest that breaching may never come to an end.

A Nurse's Practice Environment. According to the study participants, a nurse's practice environment can be assumed to be made up of a complex and often unpredictable set of activities. The level of complexity could determine unanticipatedly, how the nurse navigates patient information privacy. This practice environment has not been well studied and documented.

Patient Information Privacy and Security Nursing Experiences. Although the patient's information privacy regulations had to be followed, the nurse's experiences in this area were not bound by these regulations. Experiences as conveyed by the nurses consisted of a boundless mirage of feelings, reflections, thoughts, suggestions, apprehensions, comprehension, etc. that influenced the nurse's day-to-day actions or were the results of his or her actions.

Patient Information. The literature provides a technical definition of what patient information is. In an article written by the University of Illinois Chicago (2020), the author defines patient information simply to include a range of different data types such as patient's medical history, medical test results, and insurance information. In this exploratory study however, this list was intuitively extended by the nurses to include confidential personal information divulged to the nurse during hospitalization, close family (children and spouse) information, etc.

The Nurse. For the purposes of this study, the nurse was presumed to be prepared to take control of situations, be decisive, and capable of handling all manner of nursing practice nuances, including matters concerning patient information privacy and security. The nurse was also described as being dichotomously a protector and liberator of information, and a believer in the flexibility of information availability. The nurse's desire for information was sometimes described as being "overpowering". He or she was described as capable of exercising restraint and is disciplined, while at the same time disliking bureaucracy and has the tendency to not follow the rules. The complexity of the person of a nurse was further elaborated when she or he was perceived as having "dual perspective" since at some point, the nurse was a patient giving information, but now receiving information.

Nurse-Patient Family Relationship. Assumptions each of these parties (Nurses and Patient's Family) made regarding patient information was perhaps part of the major reason for the adversarial relationship which possibly let some nurses describe patient family challenges as one of the worse situations that nurses had to deal with. The patient's family assumed that the nurse knew everything going on with the patient but refused to share. The family members also

felt entitled to every information about the patient. The nurse perhaps thought the family members were aware of patient information sharing restrictions they have. This area would require further investigations.

Regulatory Compliance. The phrase, “regulatory compliance” as used in the study was often in association with laws, regulations, guidelines, codes of ethics, rules, etc. that govern the use of patient information. When it came to regulatory compliance, the nurses admitted that sometimes their own humanity was in the way, making them “slip” here and there and not be compliant. They did not shy away from indicating that the same regulations may mean different things to different nurses, particularly, the younger ones. They attributed this situation to the fact that often, the laws and regulations are written by or under the guidance of legal practitioners sometimes using terms and language only trained lawyers would fully understand. Some believed that more education and training in this area would help.

7.4.2 Significance of the Study

My interest in this study came about as mentioned in Chapter 1 due to an opportunity I had as the Dean of a technical institution in the United States of America, to visit nursing students in a hospital environment. Observations I made during this visit had me asking a number of questions regarding the privacy and security of patient information. I could hardly stop thinking about this as the days went by. My professional background is from graduate degrees in forest management, business administration, and information systems security management, and this doctoral PhD is in interdisciplinary studies.

The significance of this study has some broad as well as narrow implications for nurses and nursing administrators, including implications that policy and decision makers can use. Upon dissemination of the outcomes of the study, it will enable society at large to better understand certain behaviours as they encounter nurses in a hospital environment. Nurses could also derive some comfort from knowing that society understands their perspective. This understanding could foster the necessary cordial relationship between nurses and the families of patients. This is particularly important as the nurses clearly indicated during the study that nurse-patient family relations when it came to patient information, was often one of the challenging areas for nurses. In the published literature, not much has been done to attempt to understand the nurse's "world" of regulatory compliance and the ever-changing practice environment of nurses. Results of the study provided part of this missing link. For, example, we now know a little more about how nurses feel and/or think about what they consider to be too much regulation. The research study provided the opportunity to delve into the nurses' experiences to discover what they have observed, encountered, undergone, and essentially travel their journey in the course of time, "from the horse's own mouth". The nurses would feel heard not through hearsay but empirical data, thus adding credibility and authenticity. The study has unraveled significant concerns that nurses have in many areas of patient information and provided some rationale for addressing these concerns. Outcomes of the study do not only have serious implications for patient information and security policy formulation and updates, but also provides a bottom-up approach to handling such policies.

What were interpreted from the data that eventually became over-arching themes were "Protection of Patient Information" and "Violations or Breaches of Patient Information". These

led to subthemes or factors that either secured or breached patient information, and have been previously discussed. Also significant in the findings were what the nurses said and how they felt. These utterances and feelings were descriptive of what was going on in their nursing lives regarding patient information privacy and security. A lot has been learned from the nurses' apprehensions, information system use, and information sharing practices, information protection initiatives, attitudes toward patient information, beliefs and perceptions, ascribed meanings, thinking and interpretations, like and dislike for bureaucracy. Other areas where a great deal was revealed in this study pertained to breaches. These included: purposive and unintentional breaches; reasons for violations; the nurse's thoughts, feelings and understanding of a breach; types of breaches; attitudes towards breaches; curiosity as a special case for breaches; lack of explicit gate keeping when it came to breaches; and, breaches as a result of nursing practices.

The nurses' portrayal of "their world" as it relates to patient information privacy fit in well with the interpretive description (Thorne, 2008, 2016) theoretical foundation of this study. As interpretive description was the methodology used for this exploratory study, the following new definitions as described by the nurses were interpreted or co-constructed from the data:

Table 7.1 New Definitions

New Definitions Interpreted or Co-Constructed from the Data
Patient Information Privacy: Patient information is defined as confidential health and personal information the patient has the right to keep private, except for in "need to know" health situations where that information is entrusted to health care professionals (physicians, nurses, etc.) for the purpose of treatment and care of their physical and mental health. The

terms patient information security and safety are subsumed by the definition of patient information privacy and the terms used interchangeably (Sackey et al., 2020).

Patient Information Breach: A breach of patient information is defined as the intentional or unintentional violation of a mandated set of rules for access, retention and dissemination of patient information, due to lack of awareness or unclear consequences or deterrents (Sackey et al., 2020).

Nurse's Role in Patient Information Privacy/Breach: Professionally, nurses must follow patient information privacy acts, regulations, and mandates. Nurses most often are in the confidant or trusted position of protector, liberator, and custodian of patient information; therefore, nurses must be careful not to violate or breach patient information (Sackey et al., 2020).

References

- Alberta Health and Wellness. (1999, May). *Health Professions Act: A new law for regulated health care professionals.* <https://open.alberta.ca/dataset/0fc1ed78-4ac6-4af5-9be6-e3224c082d48/resource/c13ad967-ee21-4161-8a5b-2e85a47123f5/download/Health-Professions-Act.pdf>
- Alberta Institute of Health Economics. (2008). *Effective communication of findings from research.* http://www.ihe.ca/documents/Dissemination_0.pdf
- Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory and crowding.* Cole Pub. Co., Inc.
- Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33(3), 66–84. <https://doi.org/10.1111/j.1540-4560.1977.tb01883.x>
- American Association of Critical Care Nurses. (2008). *Moral distress.* http://www.aacn.org/WD/Practice/Docs/Moral_Distress.pdf
- American Psychiatric Association. (2008). *Testimony of the American Psychiatric Association regarding “Cost and confidentiality: The unforeseen challenges of electronic health records in small specialty practices.* <http://www.house.gov/smbiz/hearings/hearing-7-31-08-records/Plovnick.pdf>
- American Society for Bioethics and Humanities. (2011). *Core competencies for healthcare ethics consultation* (2nd ed.). <https://doi.org/10.1080/15265161.2012.750388>
- Anderson J. G. (2000). Security of the distributed electronic patient record: A case-based approach to identifying policy issues. *International Journal of Medical Informatics*, 60(2). [https://doi.org/10.1016/s1386-5056\(00\)00110-6](https://doi.org/10.1016/s1386-5056(00)00110-6)

- Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), 339–370. <https://doi:10.2307/20650295>
- Ardito, S. A. (2014). Electronic health records: How the conversion of print medical records could transform the healthcare industry. *Online Searcher*, 38(6), 38–44.
<http://pqasb.pqarchiver.com/infotoday/doc/1626508410.html?FMT=ABS&FMTS=ABS&FT:PAGE&type=current&date=Nov%2FDec+2014&author=Ardito%2C+Stephanie+C&pub=Online+Searcher&edition=&startpage=38-44&desc=Electronic+Health+Records>
- Asia-Pacific Economic Cooperation Secretariat. (2005). *APEC privacy framework*.
http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
- Backett, K. C., & Davison, C. (1995). Lifecourse and lifestyle: The social and cultural location of health behaviors. *Social Science & Medicine*, 40(5), 629–638.
[https://doi.org/10.1016/0277-9536\(95\)80007-7](https://doi.org/10.1016/0277-9536(95)80007-7)
- Ball, M. J., Smith, C., & Bakalar, R. S. (2007). *Personal health records: Empowering consumers*. http://www.researchgate.net/publication/6505381_Personal_health_records_empoweringconsumers
- Baltzan, P. (2019). *Business driven information systems* (6th ed.). McGraw Hill Education.
- Bamberger, K. A., & Mulligan D. K. (2010). Privacy on the books and on the ground. *Stanford Law Review*, 63(2), 247–315. <http://scholarship.law.berkeley.edu/facpubs/1305>
- Barrows, R. C., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association*, 3(2), 139–148.

<https://doi.org/10.1136/jamia.1996.96236282>

Barry, J., & Hardiker N. (2012). Advancing nursing practice through social media: A global perspective. *Online Journal of Issues in Nursing*, 17(3), 1–12.

<https://doi.org/10.3912/OJIN.Vol17No03Man05/>

Benner, P. (1984). From novice to expert: *Excellence in clinical nursing practice*. Addison-Wesley.

Biton, V., & Tabak N. (2003). The relationship between the application of nursing ethical code and nurses' work satisfaction. *International Journal of Nursing Practice*, 9, 140–157.

<https://doi.org/10.1046/j.1440-172X.2003.00418.x>

Braga, M., Ward, L., & Culbert, A. (2018). *Thousands of patient records held for ransom in Ontario home care data breach, attackers claim*.

<https://www.cbc.ca/news/technology/carepartners-data-breach-ransom-patients-medical-records-1.4749515>

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>

British Columbia College of Nursing Professionals. (2018). *Position statement: Social media use: Common expectations for nurses*.

<https://www.bccnm.ca/NP/StandardResources/INRCSocialMediaUseCommonExpectforNurses.pdf#search=Professionalism%2C%20nurses>

Buckovich, S. A., Rippen H. E., & Rozen M. J. (1999). Driving toward guiding principles: A goal for privacy, confidentiality, and security of health information. *Journal of the*

American Medical Informatics Association, 6(2), 122–133.

<https://doi.org/10.1136/jamia.1999.0060122>

Burnard, P., Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Analyzing and presenting qualitative data. *British Dental Journal*, 204(8) 429–432.

[https://doi.org 10.1038/sj.bdj.2008.292](https://doi.org/10.1038/sj.bdj.2008.292)

Calgary Herald. (2014). *Ca: AHS contacting nearly 250 patients after privacy breached*.

<http://www.phiprivacy.net/ca-ahs-contacting-nearly-250-patients-after-privacy-breached/>

Canada Health Infoway. (2007). *Electronic Health Information and Privacy Survey: What Canadians think—2007*. EKOS Research Associates.

<https://www.infoway-inforoute.ca/en/component/tags/tag/300-ekos>

Canada Health Infoway. (2008). *A “conceptual privacy impact assessment (PIA) on Canada’s electronic health record solution (EHRS) blueprint version 2*. <https://www.infoway-inforoute.ca/en/>

Canada Health Infoway. (2021). *Privacy*.

<https://www.infoway-inforoute.ca/en/solutions/implementation-support/privacy>

Canada Health Infoway, Health Canada, & Office of the Privacy Commissioner of Canada

(2007). *Electronic health information and privacy survey: What Canadians think – 2007*.

<http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/health/2007/522-06-e/report.pdf>

Canadian Association of Schools of Nursing. (2012). CASN entry-to-practice nursing informatics competencies for registered nurses. *CASN and Canada Health Infoway*.

<https://www.casn.ca/2014/12/casn-entry-practice-nursing-informatics-competencies/>

Canadian Broadcasting Corporation. (2020a). *Hospitals 'overwhelmed' by cyberattacks fuelled*

by booming black market. <https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422>

Canadian Broadcasting Corporation. (2020b). *Privacy commissioner calls for changes, consultation on health information bill.*

<https://www.cbc.ca/news/canada/edmonton/privacy-commissioner-calls-for-changes-consultation-on-health-information-bill-1.5802178>

Canada Broadcasting Corporation News. (2012). *Five employees fired after Eastern Health privacy breaches.* <http://news.ca.msn.com/local/newfoundland/5-employees-fired-after-eastern-health-privacy-breaches>

Canadian Nurses Association. (2008). *Code of ethics for registered nurses.*
http://www2.cna-aiic.ca/CNA/documents/pdf/publications/Code_of_Ethics_2008_e.pdf

Canadian Nurses Association. (2015). *The practice of nursing.*
<https://www.cna-aiic.ca/en/nursing-practice/the-practice-of-nursing>

Canadian Nurses Association. (2017). *Code of ethics for registered nurses.*
<https://www.cna-aiic.ca/~/media/cna/page-content/pdf-en/code-of-ethics-2017-edition-secure-interactive>

Canadian Nurses Protective Society. (2008). *New developments in privacy law.*
<http://www.cnps.ca/index.php?page=109>

Canadian Nurses Protective Society. (2010). Social media. *Info LAW*, 19(3).

Canadian Nurses Protective Society. (2020). *Confidentiality and privacy.*
https://cnps.ca/education_topic/confidentiality-and-privacy/

Cavoukian, A., & Rossos, P. J. (2009). *Personal health information: A practical tool for*

physicians transitioning from paper-based records to electronic health records.

<https://www.ipc.on.ca/images/Resources/phipa-toolforphysicians.pdf>

Centers for Medicare and Medicaid Services. (2008). *Security standard overview: Regulations.*

<http://www.cms.hhs.gov/Security/Standard>

Central Connecticut State University. (2013). *Focus group hints.*

http://www.ccsu.edu/uploaded/departments/AdministrativeDepartments/Institutional_Research_and_Assessment/Assessment/Resources/FocusGroupsHints.pdf

Chalmers J., & Muir R. (2003). Patient privacy and confidentiality. *British Medical Journal*, 325, 725–726. <https://doi.org/10.1136/bmj.326.7392.725>

Choi Y. B., Capitan K. E., Krause J. S., & Streeper M. M. (2006). Challenges associated with privacy in health care industry: Implementation of HIPAA and security rules. *Journal of Medical Systems*, 30(1), 57–64. <https://doi.org/10.1007/s10916-006-7405-0>

Chronicle Live. (2015). *New Castle nurse sacked after snooping on medical records and discussing them on social media.* <http://www.chroniclelive.co.uk/news/north-east-news/newcastle-nurse-sacked-after-snooping-8581684>

City News. (2015). *Personal medical records found strewn along street in Richmond Hill.* <http://www.phiprivacy.net/ca-personal-mdeical-records-found-strewn-along-street-in-richmond-hill/>

Clark, M. (2020). Real-world examples of social media HIPAA violations. *Etactics*. <https://etactics.com/blog/social-media-hipaa-violations>

Clarke, V., & Braun, V. (2013). Teaching thematic analysis. *The Psychologist*, 26(2), 120–123.

[http://eprints.uwe.ac.uk/21155/3/Teaching%20thematic%20analysis%20Research%20Re
pository%20version.pdf](http://eprints.uwe.ac.uk/21155/3/Teaching%20thematic%20analysis%20Research%20Repository%20version.pdf)

College and Association of Registered Nurses of Alberta. (2014). *CARNA Privacy Guide*.

<http://www.nurses.ab.ca/privacy/>

College and Association of Registered Nurses of Alberta. (2020a). *Employment at CARNA*.

<https://nurses.ab.ca/contact-us/careers/employment-at-carna>

College and Association of Registered Nurses of Alberta. (2020b). *Privacy and management of
health information standards*. [https://nurses.ab.ca/docs/default-source/document-](https://nurses.ab.ca/docs/default-source/document-library/standards/privacy-and-management-of-health-information-standards.pdf?sfvrsn=846398c_10)

[library/standards/privacy-and-management-of-health-information-
standards.pdf?sfvrsn=846398c_10](#)

College of Registered Nurses of Manitoba. (2020). *Practice expectation spotlight:*

Registered nurse responsibilities related to professional practice issues.

<https://www.crnmb.ca/connect/nurselink/read,article/38/practice-expectation-spotlight>

Corbin, J., & Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for
developing grounded theory*. Sage. <https://doi.org/10.4135/9781452230153>

Cornell P., Herrin-Griffith D., Keim C., Petshconeck S., Sanders A. M., D'Mello S., Golden T.
W., & Shepherd G. (2010). Transforming nursing workflow, part 1: The chaotic nature of
nursing activities. *Journal of Nursing Administration*, 40(9), 366–373. <https://doi.org/10.1097/NNA.0b013e3181ee4261>.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods
approaches* (4th ed.). Sage.

Culnan, M., & Williams C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly* 33(4), 673–687.

<https://doi.org/10.2307/20650322>

Daher, M., Carre, D., Jaramillo, A., Olivares, H., & Tomicic, A. (2017). Experience and meaning in qualitative research: A conceptual review and a methodological device proposal.

Forum for Qualitative Research, 18(3). <https://www.qualitative-research.net/index.php/fqs/article/view/2696>

Darlaston-Jones, D. (2007). Making connections: The relationship between epistemology and research methods. *The Australian Community Psychologist*, 19(1), 19–26.

[http://www.groups.psychology.org.au/Assets/Files/ACP_19\(1\).pdf#page=19](http://www.groups.psychology.org.au/Assets/Files/ACP_19(1).pdf#page=19)

Davidson, J. (2009). Electronic medical records: What they are and how they will revolutionize the delivery of resident care. *Canadian Nursing Home*, 20(3), 15–18.

Davis, J. (2020). *The 10 biggest healthcare data breaches of 2019, so far.*

<https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far>

Department of Health and Human Services. (2008). *Health information technology. Federal activities.* <http://www.hhs.gov/healthit/privacy/federal.html>

Dicicco-Bloom, B., & Crabtree, B., F. (2006). The qualitative research interview. *Medical Education*, 40, 314–321.

Edwards, E. (2013). Electronic record-keeping: Potential benefits and reasons for caution. *British Journal of Neuroscience Nursing*, 9(5), 252–253.

<https://doi.org/10.12968/bjnn.2013.9.5.213>

El-Emam, K., Jonker, E., Arbuckle, L., & Malin, B. (2011). A systematic review of re-

- identification attacks on health data. *Plos One*, 6(12) 1–12.
<http://www.plosone.org/article/fetchObject.action?uri=info%3Adoi%2F10.1371%2Fjournal.pone.0028071&representation=PDF>
- Elliott, S. J., & Gillie, J. (1998). Moving experiences: A qualitative analysis of health and migration. *Health & Place*, 4(4), 327–339.
- Erickson, J. I., & Millar, S. (2005). Caring for patients while respecting their privacy: Renewing our commitment. *ANA Periodicals*, 10(2).
- http://ojin.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Volume102005/No2May05/tpc27_116017.html
- Erlich, H. S. (2008). Experience – what is it? *International Journal of Psychoanalysis*, 84(5), 1125–1147. <https://doi.org/10.1516/6HJ2-WKWW-6EYX-EYAA>
- Federal Trade Commission. (2012). *Google will pay \$22.5 million to settle FTC charges it.* <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>
- Fenton, W. (2006). Developing a guide to improve the quality of nurses' handover. *Nursing Older People*, 18(11), 32–36. <https://doi.org/10.7748/nop.18.11.32.s24>
- Field Law. (2020). *Alberta's health information act: What is changing?* <https://www.mondaq.com/canada/privacy-protection/1004270/alberta39s-health-information-act-what-is-changing>
- Fionda, F. (2019). *Pager systems used in healthcare could be exposing patient data across Canada.* <https://www.ctvnews.ca/health/pager-systems-used-in-healthcare-could-be-exposing-patient-data-across-canada-1.4727129>

Foreman, T. M., Armor, D. A., & Miller, A. S. (2020). A review of clinical informatics competencies in nursing to inform best practices in education and nurse faculty development. *Nursing Education Perspectives*, 41(1), E3–E7.

<https://doi.org/10.1097/01.NEP.0000000000000588>

ForgeRock. (2020). *ForgeRock consumer identity breach report*.
<https://www.forgerock.com/resources/view/107130151/analyst-report/forgrock-consumer-identity-breach-report.pdf>

Forrester Research. (2013). *Measure the effectiveness of your data privacy program*.
<https://www.forrester.com/Measure+The+Effectiveness+Of+Your+Data+Privacy+Program/fulltext/-/E-RES61553>

Garets, D., & Davis, M. (2006). *Electronic medical records vs. electronic health records: Yes, there is a difference. A HIMSS analytics white paper*.
file:///C:/Users/aeK587/AppData/Local/Microsoft/Windows/INetCache/IE/0MBACKW6/EMR%20vs%20EHR.pdf

Gaston Gazette. (2015). *Nurse pastor's wife pleads guilty to identity theft*.
<http://www.gastongazette.com/20150306/nurse-pastors-wife-pleads-guilty-to-id-theft-303069932>

Geertz, C. (1973). *The interpretation of cultures*.
[https://books.google.ca/books?id=34yKDgAAQBAJ&dq=GEERTZ+C+\(1973\)+The+Interpretation+of+Culture+Basic+Books,+New+York&lr=](https://books.google.ca/books?id=34yKDgAAQBAJ&dq=GEERTZ+C+(1973)+The+Interpretation+of+Culture+Basic+Books,+New+York&lr=)

Gellman, R. (2015). *Fair information practices: A brief history*.
<http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>

Glaser, B., & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine Transaction.

Glaser, B. G., & Strauss, A. L. (1999). *The discovery of grounded theory: Strategies for qualitative research*. Aldine Transaction.

Global News. (2014). *Edmonton man outraged after information breach by a city hospital*.

<http://www.globalnews.ca/1608295/>

edmonton-man-outraged-after-information-breach-by-a-city-hospital/

Global News. (2015). *Privacy breach of patient records in Prince Albert health region*.

<http://www.globalnews.ca/news/1800984/privacy-breach-of-patient-records-in->

Globe and Mail. (2014). *Jack Layton's hospital records were also accessed, Chow says*.

<http://www.theglobeandmail.com/news/toronto/jack-laytons-hospital-records-were-also-accessed-chow-says/article21154944/>

Glowingwlg.com. (2018). *New mandatory breach reporting under the Alberta Health Information Act*. <https://gowingwlg.com/en/insights-resources/articles/2018/new-mandatory-breach-reporting-under-the-alberta-h/>

Government of Alberta. (2020a). *Health Information Act*. Information. Alberta Queen's Printer
<https://www.alberta.ca/health-information-act.aspx>

Government of Alberta. (2020b, June 26). *Health Information Act*. Province of Alberta
[Revised Statutes of Alberta 2000 Chapter H-5 Current as of June 26, 2020]
Alberta Queen's Printer. <https://www.qp.alberta.ca/documents/Acts/H05.pdf>

Government of Canada. (2020a). *Personal Information Protection and Electronic*

Documents Act. [S.C. 2000, c. 5; Act current to 2020-12-02, last amended 2019-06-21].

Justice Laws Website. <http://laws-lois.justice.gc.ca/eng/acts/p-8.6/>

Government of Canada. (2020b). *The Personal Information Protection and Electronic*

Documents Act, 2000. <http://laws-lois.justice.gc.ca/eng/acts/p-8.6/>

Government of Saskatchewan. (2020a). *The Health Information Protection Act.* [Effective

September 1, 2003, with amendments by the Statutes of Saskatchewan to 2020]. The

Queen's Printer. <http://www.qp.gov.sk.ca/documents/english/Statutes/Statutes/H0->

021.pdf

Government of Saskatchewan. (2020b). *Your personal health information and privacy*

<https://www.saskatchewan.ca/residents/health/accessing-health-care-services/your->

personal-health-information-and-privacy

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N.

K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 105–117).

Sage.

Guest, G., MacQueen, K., & Namey, E. (2012). *Applied thematic analysis.* Sage.

Guest, G., Namey, E., & Mitchell, M. (2013). *Collecting qualitative data: A field manual for applied research.* Sage.

Hayrinien, K., Saranto, K., & Nykanen, P. (2007). Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International*

Journal of Medical Information, 77(5), 291–304. <https://doi.org/10.1016/j.ijmedinf.2007.09.001/>

HealthCare IT News. (2013). *Nurses' gossip uncovers privacy breach. Nurse sacked for*

snooping in patient files. <http://www.healthcareitnews.com/news/nurse%20%99s-gossip-uncovers-privacy-breach>

HealthIT. (2018). *What are electronic health records (EHRs)?*
<https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-are-electronic-health-records-ehrs>

HealthIT. (2019). *What is an electronic health record (EHR)?*

<https://www.healthit.gov/faq/what-electronic-health-record-ehr>

HealthIT. (2020). *Personal health record (PHR).* TechTarget.

<https://searchhealthit.techtarget.com/definition/personal-health-record-PHR>

Hebert, P. C., Flegel, K., Stanbrook, M. B., & MacDonald, N. (2010). No privacy of health information in Canada's armed forces. *Canadian Medical Association Journal, 183*(3). 167–168. <https://doi.org/10.1503/cmaj.101630>

Herald Tribune. (2014). *ER nurse fired, accused of using patients' credit card info.*
<http://www.heraldtribune.com/article/20141210/breaking/141219994/2055/News?Title=ER-nurse-fired-accused-of-using-patients-credit-card-info>

Hsiao, C-J., & Hing, E. (2014). Use and characteristics of electronic health record systems among office-based physician practices: United States, 2001–2013. *National Center for Health Statistics, 143*, 1–8.

Informa Healthcare. (2009). Electronic health records and privacy. *Issues in Mental Health Nursing, 30*, 408–409.

International Standards Organization. (2013). *ISO/IEC 27001 – Information security management.*

- <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>
- Iowa Board of Nursing. (2014). The internet, television, social media, and nursing: Understand your professional responsibility. *Iowa Board of Nursing Newsletter*, 33(1), 1–2.
http://publications.iowa.gov/16313/1/IBN2_14.pdf
- Jabareen, Y. (2009). Building a conceptual framework: Philosophies, definitions, and procedures. *International Journal of Qualitative Methods*, 8(4), 49–62.
<https://doi.org/10.1177/160940690900800406>
- Jacob, S., A., & Furgerson, S., A. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *The Qualitative Report*, 17(6), 1–10. <https://nsuworks.nova.edu/tqr/vol17/iss42/3>
- Jain, A., & Ogden, J. (1999). General practitioners' experiences of patients' complaints: Qualitative study. *British Medical Journal*, 318, 1596–1599. <https://doi.org/10.1136/bmj.318.7198.1596>
- Jangland, E., & Larsson, J. (2011). Surgical nurses' different understandings of their interactions with patients: A phenomenographic study. *Scandinavian Journal of Caring Sciences*, 25(3), 533–541. <https://doi.org/10.1111/j.1471-6712.2010.00860.x>
- Kamerer, J. L., & McDermott (2020). Cybersecurity: Nurses on the front line of prevention and= education. *Journal of Nursing Regulation*, 10(4), 48–53.
[https://doi.org/10.1016/S2155-8256\(20\)30014-4](https://doi.org/10.1016/S2155-8256(20)30014-4)
- Kane B., & Sands D. Z. (1998). Guidelines for the clinical use of electronic mail. *Journal of the*

American Medical Informatics Association, 5(1), 104–111. <https://doi.org/10.1136/jamia.1998.0050104>

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59–68. <https://doi.org/10.1016/j.bushor.2009.09.003>

Kent-Wilkinson A. (2008). *Forensic nursing education in North America: An exploratory study*. Dissertation submitted to the College of Graduate Studies and Research in partial fulfillment of the requirement for the degree of Doctor of Philosophy, Department of Education Administration, University of Saskatchewan, Saskatoon, SK, Canada.

<https://doi:10.1111/j.1939-3938.2009.01055.x>

Kerr, H., Booth, R., & Jackson, K. (2020). Exploring the characteristics and behaviors of nurses who have attained microcelebrity status on Instagram: Content analysis. *Journal of Medical Internet Research*, 22(5). <https://doi:10.2196/16540>

Kerse, N., Thomas, D. R., Neuwelt, P., Crampton, P., Dixon, R., & Dyall, L. (2004). *Consumers' views and experiences of primary health care in New Zealand: A snapshot*. Ministry of Health.

Kitto, S. C., Chesters, J. & Grbich, C. (2008). Quality in qualitative research: Criteria for authors and assessors in the submission and assessment of qualitative research articles for the Medical Journal of Australia. *Medical Journal of Australia*, 188, 243–246.

<https://doi.org/10.5694/j.1326-5377.2008.tb01595.x>

- Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management* 41(5), 597–607.
- Kutney-Lee, A., McHugh, M. D., Sloane, D. M., Cimiotti, J. P., Flynn, L., Neff, D. F., & Aiken, L. H. (2009). *Nursing: A key to patient satisfaction*.
<https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.28.4.w669>
- Langland, E., Larsson, J., & Gunningberg, L. (2010). Surgical nurses' different understandings of their interactions with patients: A phenomenographic study. *Scandinavian Journal of Caring Sciences*, 25(3), 533–541. <https://doi.org/10.1111/j.1471-6712.2010.00860.x>
- Larsson, I. E., Sahlsten, M., Segesten, K., & Plos, K. A. E. (2011). *Patients' perceptions of nurses' behaviour that Influence patient participation in nursing care: A critical incident study*. Nursing Research and Practice.
<http://downloads.hindawi.com/journals/nrp/2011/534060.pdf>
- Latimer, K. (2018). Privacy commissioner still waiting two years later for amendments to health information privacy laws. *Canadian Broadcasting Corporation News*.
<https://www.cbc.ca/news/canada/saskatchewan/sask-privacy-commissioner-annual-report-1.4714557>
- Laudon, K. C., & Laudon, J. P. (2014). *Management information systems. Managing the digital firm* (7th ed., pp. 4–25). Pearson.
- Lavatto, K. (2014). National nurses' week highlights the many leadership roles of nurses. *Medsurg Nursing*, 23(4), 141–142.
- Leadgenera.com. (2020). *The 10 best social media and content apps for 2020*.

<https://leadgenera.com/knowledge-hub/the-10-best-social-media-and-content-apps-for-2020/>

Leininger, M. M. (1984). *The essence of nursing and health*. Slack.

Leino-Kilpi, H., Valimaki, M., Dassen, T., Gasull, M., & Lemonidou, C. (2001). Privacy: A review of the literature. *International Journal of Nursing Studies*, 36(8), 663–671.

[https://doi.org/10.1016/s0020-7489\(00\)00111-5](https://doi.org/10.1016/s0020-7489(00)00111-5)

Ludwick, D. A., & Doucette, J. (2009). Adopting electronic medical records in primary care: Lessons learned from health information systems implementation experience in seven countries. *International Journal of Medical Informatics*, 78, 22–31. <https://doi.org/10.1016/j.ijmedinf.2008.06.005>

Malin, B. A., Emam, K. E., & O’Keefe, C. M. (2013). Biomedical data privacy: Problems, perspectives, and recent advances. *Journal of American Medical Association*, 20(1), 2–6
<https://doi.org/10.1136/amiajnl-2012-001509>

Mandl, K. D., Szolovits, P., & Kohane, I. S. (2001). Public standards and patients’ control: How to electronic medical records accessible but private. *British Medical Journal*, 322, 283–287. <https://doi.org/10.1136/bmj.322.7281.283>

Marshall, M. N. (1999). Improving quality in general practice: Qualitative case study of barriers faced by health authorities. *British Medical Journal*, 319, 164–167.
<https://doi.org/10.1136/bmj.319.7203.164>

McKenna, L. (1997). Improving the nursing handover report. *Professional Nurse*, 12(9), 637–639.

Metro News. (2015). *CA: Newfoundland patient data breach investigated (updated)*.

<http://www.databreaches.net/ca-newfoundland-patient-data-breach-investigated/>

Moore, J. H. (1997). *Towards a theory of privacy in the information age.*

<http://www.site.uottawa.ca/~stan/csi2911/moor2.pdf>

Nagle, L. M., Kleib, M., & Furlong, K. (2020). Digital health in Canadian schools of nursing

Part A: Nurse educators' perspectives. *Quality Advancement in Nursing Education -*

Avancées en formation infirmière, 6(1), Article 4, 1–17.

<https://doi.org/10.17483/2368-6669.1229>

National Council of State Boards of Nursing. (2011). White paper: A nurse's guide to the use of

social media. https://www.ncsbn.org/11_NCSBN_Nurses_Guide_Social_Media.pdf

National Council of State Boards of Nursing. (2012). *Social media guidelines for nurses.*

<https://www.ncsbn.org/347.htm>

National Council of State Boards of Nursing Inc. (2018). *A nurse's guide to the use of social*

media. https://www.ncsbn.org/NCSBN_SocialMedia.pdf

National Institute of Standards in Technology. (2015). Electronic health records on mobile

devices. https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices

National Law Review (2020). Privacy & data security: 2020 considerations for the Insurance

industry. <https://www.natlawreview.com/article/privacy-data-security-2020-considerations-insurance-industry>.

National Public Radio. (2015). *The black market for stolen health care data.*

<http://www.phiprivacy.net/the-black-market-for-stolen-health-care-data/>

New York Times. (2019). *Google to store and analyze millions of health records.*

- <https://www.nytimes.com/2019/11/11/business/google-ascension-health-data.html>
- NielsonWire. (2010). *Social networks/blogs now account for one in every four and a half minutes online.* <http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online>
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and integrity of social life.* https://crypto.stanford.edu/portia/papers/privacy_in_context.pdf
- North Bay Local News. (2011). *Nurse fired after breach of privacy at hospital.* <http://www.nugget.ca/2011/09/06/nurse-fired-breach-of-privacy-at-hospital>
- North York Mirror. (2014). *North York hospitals post notices to patients after privacy breach.* <http://www.insidetoronto.com/news-story/4840921-north-york-hospitals-post-notices-to-patients-after-privacy-breach/>
- Northumberland News. (2014). *Lakeridge Health reports 578 patient records inappropriately accessed.* <http://www.northumberlandnews.com/news-story/5159653-lakeridge-health-reports-578-patient-records-inappropriately-accessed/>
- Nurses Association of New Brunswick. (2012). *Practice guideline: Ethical and responsible use of social media technologies.* [http://www.nanb.nb.ca/downloads/Practice%20Guidelines-%20Social%20Media-E\(1\).pdf](http://www.nanb.nb.ca/downloads/Practice%20Guidelines-%20Social%20Media-E(1).pdf)
- Nursing and Midwifery Board of Australia. (2010). *Information sheet on social media.* <http://www.nursingmidwiferyboard.gov.au/Codes-Guidelines-Statements/FAQ.aspx>
- Nursing and Midwifery Council. (2011). *Social networking site.* <http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/>
- Office of Inadequate Security. (2015). *Healthfirst notifying 5,300 members whose data were*

stolen between 2012 and 2014. <http://www.databreaches.net/healthfirst-notifying-5300-members-whose-data-were-stolen-between-2012-2014/prince-albert-health-region/>

Office of the Privacy Commissioner of Canada. (2011). *2011 Canadians and privacy survey report.* https://www.priv.gc.ca/information/por-rop/2011/por_2011_01_e.pdf

Office of the Privacy Commissioner of Canada. (2013). *Survey of Canadians on privacy-related issues.* https://www.priv.gc.ca/media/3323/por_2013_01_e.pdf

Office of the Privacy Commissioner of Canada. (2018). *Summary of privacy laws in Canada.* https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Office of the Privacy Commissioner of Canada. (2019). *2018-19 survey of Canadians on privacy.* https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/

Ohio Nurses Association. (2013). What do I do now? Ethical dilemmas in nursing and healthcare. *ISNA Bulletin*, 5–12.

<http://www.thefreelibrary.com/What+do+I+do+now%3F+Ethical+dilemmas+in+nursing+and+health+care.-a0323972766>

Organization for Economic Cooperation and Development. (2010). *OECD privacy principles.* <http://oecdprivacy.org/>

Orlikowski, W. J., & Baroudi, J. J. (1991). *Studying information technology in organizations: Research approaches and assumptions.*

<https://archive.nyu.edu/bitstream/2451/14404/1/IS-90-04.pdf>

Palen, L., & Dourish, P. (2003). Unpacking “privacy” for a networked world. *Privacy and Trust,*

5(1), 129–136.

Park, M. (2009). Ethical issues in nursing practice. *Journal of Nursing Law*, 13(3), 68–77.

<https://doi.org/10.1891/1073-7472.13.3.68>

Parks, R., Chu C., & Xu H. (2011). Healthcare information privacy research: Issues, gaps, what next? *Healthcare Information Privacy Research. Americas Conference on Information Systems 2011 proceedings*.

Perera, G., Holbrook, A., Thabane, L., Foster, G., & Willison, D. J. (2011). Views on health information sharing and privacy from primary care practices using electronic medical records. *International Journal of Medical Informatics*, 80, 94–101. <https://doi.org/10.1016/j.ijmedinf.2010.11.005>

Phillips, J. (2020). Local legislation impacts nursing and those we serve. *Minority Nurse*. <https://minoritynurse.com/local-legislation-impacts-nursing-and-those-we-serve/>

Privacy Rights Clearinghouse. (2012). *Personal health records and privacy*. <https://www.privacyrights.org/fs/fsC7/CA-medical-personal-health-records>

Privacy Rights Clearinghouse. (2017). *Personal health records and your privacy*. <https://privacyrights.org/consumer-guides/personal-health-records-and-your-privacy-california-medical-privacy-series>

Privacy Rights Clearinghouse's Chronology of Data Breaches. (2015). *Chronology of data breaches*. <http://www.privacyrights.org/data-breach/newQuestionPro>. (2020). *Qualitative data – Definition, types, analysis and examples*. <https://www.questionpro.com/blog/qualitative-data/>

Radio New Zealand. (2015). *Medical files found in unused house*.

<http://www.radionz.co.nz/news/national/266339/medical-files-found-in-unused-house>

Rainer, R. K., Celgielski, C. G., Splettstoesser-Hogeterp, I., & Sanchez-Rodriguez, C.

(2011). *Introduction to information systems* (2nd ed., pp. 111–133). Wiley & Sons.

Rchaidia, L., Dierckx, de Casterle, B., De Blaeser, L., & Gastmans, C. (2009). Cancer patients' perceptions of the good nurse: A literature review. *Nursing Ethics*, 16(5), 528–542.

<https://doi.org/10.1177/0969733009106647>

Reddy, M., Pratt W., Dourish, P., & Shabot, M. M. (2003). Sociotechnical requirements analysis for clinical systems. *Methods of Information in Medicine*, 42, 437–444.

<http://doi.org/10.1055/s-0038-1634346>

Registered Nurses Association of Ontario. (2007a). *Embracing cultural diversity in health care: Developing cultural competence*. <https://rnao.ca/bpg/guidelines/embracing-cultural-diversity-health-care-developing-cultural-competence>

Registered Nurses Association of Ontario. (2007b). *Healthy work environments best practices. Professionalism in nursing*.

http://rnao.ca/sites/rnao-ca/files/Professionalism_in_Nursing.pdf

Research Information Network & Joint Information Systems Committee. (2009).

Communicating knowledge: How and why UK researchers publish and disseminate their findings.

<http://www.jisc.ac.uk/media/documents/publications/communicatingknowledgereport.pdf>

Richards, L. (2009). *Handling qualitative data. A practical guide* (2nd ed., pp. 9–33). Sage.

Richards, L., & Morse, J. M. (2013). *Read me first for a user's guide to qualitative methods* (3rd ed., pp. 61–67). Sage.

Riffkin R. (2014). *Americans rate nurses highest on honesty, ethical standards.*

<http://www.gallup.com/poll/180260/americans-rate-nurses-highest-honesty-ethical-standards.aspx>

Roberts J., Floyd S., & Thompson S. (2011). The clinical nurse specialist in New Zealand: How is the role defined? *Nursing Praxis in New Zealand*, 27(2), 24–35.

Robey, S. (2014). *Ten problems electronic records can help solve.*

<http://www.fool.com/investing/general/2014/07/19/10-problems-electronic-health-records-can-help-sol.aspx>

Rodziewicz, T. L., Houseman B., & Hipskind, J. E. (2020). *Medical error prevention.*

<https://www.ncbi.nlm.nih.gov/books/NBK499956/>

Roseman, E. (2014). *Tip leads to notification of security lapse.*

http://www.thestar.com/business/personal_finance/2014/09/09/tip-leads-to-notification-of-security-lapse-roseman.html

Rosenbaum, S., Borzi, P. C., Repasch, L., Burke, T., & Benevelli, J. F. (2005). *Charting the legal environment of health information.*

http://hsr.himmelfarb.gwu.edu/cgi/viewcontent.cgi?article=1222&context=sphhs_policy_facpubs

Royal College of Nursing. (2003). *Defining nursing.*

http://www.rcn.org.uk/__data/assets/pdf_file/0008/78569/001998.pdf

Royal College of Nursing. (2020). *Principles of nursing practice. Eight principles that apply to all nursing staff and nursing students in any care setting.*

<https://www.rcn.org.uk/professional-development/principles-of-nursing-practice>

Samarati, P., & Sweeney, L. (1998). *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression.*

https://epic.org/privacy/reidentification/Samarati_Sweeney_paper.pdf

Sandelowski, M., & Barroso, J. (2003). Writing the proposal for a qualitative research methodology project. *Qualitative Health Research, 13*(6), 782–820.

Saskatchewan Registered Nurses Association. (2015). *Better health for all through nursing regulation, professional practice, and collaboration.*

<http://www.srna.org/index.php/nursing-practice/resources>

Saskatchewan Registered Nurses Association. (2020). *About the SRNA.*

[https://www.srna.org/about-](https://www.srna.org/about-us/#:~:text=The%20Saskatchewan%20Registered%20Nurses%20Association%20is%20the%20largest%20profession%2Dled,governed%20by%20the%20SRNA%20Council.)

[us/#:~:text=The%20Saskatchewan%20Registered%20Nurses%20Association%20is%20the%20largest%20profession%2Dled,governed%20by%20the%20SRNA%20Council.](https://www.srna.org/about-us/#:~:text=The%20Saskatchewan%20Registered%20Nurses%20Association%20is%20the%20largest%20profession%2Dled,governed%20by%20the%20SRNA%20Council.)

Schers, H., van den Hoogen, H., Grol, R., & van den Bosch. (2009). Continuity of information in general practice. *Scandinavian Journal of Primary Health Care, 21*(1), 21–26.

<https://doi.org/10.1080/02813430310000519>

Semachew, A. (2018). Implementation of nursing process in clinical settings: The case of three governmental hospitals in Ethiopia, 2017. *MBC Research Notes, 11*, 173.

<https://doi.org/10.1186/s13104-018-3275-z>

Shiel, W. C. (2021). *Medical definition of patient.*

<https://www.medicinenet.com/patient/definition.htm>

Siegmund, L. A. (2020). Social media in occupational health nursing: Helpful or harmful? *PubMed.* <https://doi.org/10.1177/2165079920935779>

Smith, J. (1999). Towards a secure EPR: Cultural and educational issues. *International Journal of Medical Informatics*, 60(2), 137–142.

https://www.academia.edu/14149111/Towards_a_secure_EPR_cultural_and_educational_issues

Spector, N., & Kappel, D., M. (2012). *Guidelines for using electronic and social media: Regulatory perspective.*

<http://www.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Vol-17-2012/No3-Sept-2012/Guidelines-for-Electronic-and-Social-Media.html>

Statutes of Saskatchewan. (1988). *The Registered Nurses Act.*

<http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/R12-2.pdf>

Stoddart, J. (2012). *The right to privacy in the privacy sector.* <http://www.cha-shc.ca/english/advocacy/the-right-to-privacy-in-the-private-sector.html#sthash.3XaalGxo.dpbs>

Stolee, P., Zaza, C., Pedlar, A., & Myers, A. M. (1999). Clinical experience with goal attainment scaling in geriatric care. *Journal of Aging and Health*, 11(1), 96–124. <https://doi.org/10.1177/089826439901100106>

Stone, M. A., Redsell, S. A., Ling, J. T., & Hay, A. D. (2005). Sharing patient data: Competing demands of privacy, trust and research in primary care. *British Journal of General Practice*, 55, 783–789. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1562354/>

Sunyaev, A., Chornyi, D., Mauro, C., & Krcmar H. (2010). *Evaluation framework for*

Personal health records: Microsoft healthvault vs. Google health.

https://www.researchgate.net/publication/221177010_Evaluation_Framework_for_Personal_Health_Records_Microsoft_HealthVault_Vs_Google_Health

The Law House. (2019). *Breach*. <https://www.thelawhouse.org/legal-services/breach/>

The Peterborough Examiner. (2015). *PRHC privacy lawsuit to go ahead*.

<http://www.thepeterboroughexaminer.com/2015/02/18/prhc-privacy-lawsuit-to-go-ahead>

The Press. (2014). *Stressed nurse fined \$6K for “snooping”*.

<http://www.stuff.co.nz/the-press/10412230/stressed-nurse-fined-6k-for-snooping>

The Standard News. (2020). *Understanding the therapeutic nurse-patient relationship*.

<https://www.cno.org/en/learn-about-standards-guidelines/magazines-newsletters/the-standard/January-2020/Understanding-the-therapeutic-nurse-patient-relationship>

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data.

American Journal of Evaluation, 27(2), 237–246.

<https://doi.org/10.1177/1098214005283748>

Thorne, S. (2008). *Interpretive description: Qualitative health research*. Left Coast Press.

<https://doi.org/10.1177/1049732310374064>

Thorne, S. (2016). *Interpretive description: Qualitative research for applied practice*. Taylor & Francis Group. <https://doi.org/10.4324/9781315545196>

Thorne, S., Kirkham S. R., & O’Flynn-Magee K. (2004). *The analytic challenge in interpretive description*. <https://journals.sagepub.com/doi/pdf/10.1177/160940690400300101>

Times Colonist. (2015). *Ca: Data breach findings in limbo since 2012, legislature hears*.

<http://www.phiprivacy.net/ca-data-breach-findings-in-limbo-since-2012-legislature-hears/>

Toronto Star. (2014). *Three Greater Toronto area hospitals don't proactively audit access to patient files.*

http://www.thestar.com/news/gta/2014/12/26/star_investigation_3_gta_hospitals_dont_proactively_audit_accesstopatient_files.html#

Toronto Star. (2015a). *Hundreds of hospital privacy violations go unreported.*

http://www.thestar.com/life/health_wellness/2015/01/13/hundreds_of_hospital_privacy_violations_go_unreported_.html

Toronto Star. (2015b). *Ontario should prosecute those snooping into patients medical records.*

<http://www.phiprivacy.net/toronto-stars-view-ontario-should-prosecute-those-snooping-into-patients-medical-records/>

Tsai, J., Egelman, S., Cranor, L., & Acquisti, A. (2010). The effect of online privacy information on purchasing behavior: An experimental Study. *Information Systems Research*.

Turner, III, D., W. (2010). Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report*, 15(3), 754–760.

University of Illinois Chicago. (2020). *What is patient information, and how is it protected?*
<https://healthinformatics.uic.edu/blog/what-is-patient-information/>

Uppsala University. (2012). *Discussion paper about the theoretical foundations of PACT. Privacy and Security Research Paper Series*, 2. http://www.projectpact.eu/privacy-security-research-paper-series/%232_Privacy_and_Security_Research_Paper_Series.pdf

- Vancouver Sun. (2014). *Ca: “Curiosity” of Island Health employees led to privacy breach, probe reveals.* <http://www.phiprivacy.net/ca-curiosity-of-island-health-employees-led-to-privacy-breach-probe-reveals/>
- Ventola, C. L. (2014). Mobile devices and apps for health care professionals: Uses and benefits. *Pharmacy and Therapeutics. Journal for Managed Care and Hospital Formulary Management*, 39(5), 356–364. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126/>
- Walker, J. M., Bieber, E. J., Richards, F., & Buckley, S. (1988). Implementing an electronic health record system. *Health Informatics Series*. <https://www.springer.com/gp/book/9781846283307>
- Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, 15, 320–330. <https://doi.org/10.1057/palgrave.ejis.3000589>
- Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220. <http://www.english.illinois.edu/-people/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>
- Washington Association for Bilingual Education. (2015). *GA: Nurse indicted on health care fraud, identity theft.* <http://www.phiprivacy.net/ga-nurse-indicted-on-health-care-fraud-identity-theft/>
- Webster Dictionary. (2014). *Webster dictionary online*. Definition of experience. <http://dictionary.reference.com/browse/Experience?s=t>
- Westin, A. F. (1967). *Privacy and freedom*. <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>
- Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 291

1–35. <https://doi.org/10.1111/1540-4560.00072>

Weston, M. J. (2010). Strategies for enhancing autonomy and control over nursing practice. *The Online Journal of Issues in Nursing*, 15(1), 1–5. <https://doi.org/10.3912/OJIN.Vol15No01Man02>

Whatis.com. (2015). *Social media*.

<http://whatis.techtarget.com/search/query?q=What+is+social+media>

Wheat, K. (2009). Applying ethical principles in healthcare practice. *British Journal of Nursing*, 18(17), 1062–1063. <https://doi.org/10.12968/bjon.2009.18.17.44162>

Williams, C., Champion, T., & Hall, I. (2018). *MGMT: Principles of management* (3rd Cdn ed.). Nelson Education Ltd.

Wise, E. K., & Shorter, J. D. (2014). Social networking and the exchange of information. *Issues in Information Systems*, 15(II), 103–109. http://iacis.org/iis/2014/95_iis_2014_103-109.pdf

World Health Organization. (2020). *Year of the nurse and the midwife 2020*. <https://www.who.int/campaigns/year-of-the-nurse-and-the-midwife-2020>

Xiaoding, X., Xixi, C., & Zongfei,. L. (2019). Impacts of nursing unit design on visibility and proximity and its influences on communication, privacy, and efficiency. *Pubmed*. <https://doi.org/10.1177/1937586719881443>

Appendix 1

Behavioral Research Ethics Board Certificate of Approval



Behavioural Research Ethics Board

Certificate of Approval

PRINCIPAL INVESTIGATOR
Arlene Kent-Wilkinson

DEPARTMENT
Nursing

BEH#
15-331

INSTITUTION(S) WHERE RESEARCH WILL BE CONDUCTED

Royal University Hospital
103 Hospital Drive
Saskatoon SK S7N 0W8

Foothills Medical Centre
1403 29 St. NW
Calgary AB T2N 2T9

Red Deer Regional Hospital Centre
3942 50a Avenue
Red Deer AB T4N 4E7

STUDENT RESEARCHER(S)
Ebenezer Sackey

FUNDER(S)
UNFUNDDED

TITLE

An Exploratory Study of Registered Nurses' Experiences in Patient Information Privacy and Security within the Provinces of Alberta and Saskatchewan

ORIGINAL REVIEW DATE APPROVAL ON
02-Nov-2015 06-Jan-2016

APPROVAL OF:
Application for Behavioural Research Ethics
Review
Recruitment Poster
Letter of Invitation
Consent Form for In-person Interview
Interview Guide/Questions
Demographic Questionnaire
Data Release Form

EXPIRY DATE
05-Jan-2017

Full Board Meeting
Delegated Review

Date of Full Board Meeting:

CERTIFICATION

The University of Saskatchewan Behavioural Research Ethics Board has reviewed the above-named research project. The proposal was found to be acceptable on ethical grounds. The principal investigator has the responsibility for any other administrative or regulatory approvals that may pertain to this research project, and for ensuring that the authorized research is carried out according to the conditions outlined in the original protocol submitted for ethics review. This Certificate of Approval is valid for the above time period provided there is no change in experimental protocol or consent process or documents.

Any significant changes to your proposed method, or your consent and recruitment procedures should be reported to the Chair for Research Ethics Board consideration in advance of its implementation.

ONGOING REVIEW REQUIREMENTS

In order to receive annual renewal, a status report must be submitted to the REB Chair for Board consideration within one month prior to the current expiry date each year the study remains open, and upon study completion. Please refer to the following website for further instructions: <http://research.usask.ca/fors-researchers/ethics/index.php>

Please send all correspondence to:

Research Ethics Office
University of Saskatchewan
Box 5000 RPO University, 1602-110 Gymnasium Place
Saskatoon SK S7N 4J8
Telephone: (306) 966-2975 Fax: (306) 966-2069

Appendix 2

Invitation to Participate in a Research Study

Study Title: Exploration of nurses' experiences with patient information privacy and security in Saskatchewan and Alberta.

Dear ___,

My name is Ebenezer Sackey. I am a graduate student in the Interdisciplinary Department at the University of Saskatchewan. I am conducting a research study as part of the requirements of my degree in patient information privacy and security, and I would like to invite you to participate.

The purpose of my exploratory study is to gain insights into the experiences of medical-surgical/critical care registered nurses in patient information privacy. My goal is to understand the perceptions, thoughts, reflections, and contributions nurses have in this area of practice, and implications for regulatory/policy research in the future. If you decide to participate, you will be asked to meet with me for an interview about your personal experience about patient information privacy and security.

The meeting will take place at a mutually agreed upon time and place, and should last about 30-45 minutes. The session or interview will be audio recorded so that I can accurately reflect on what is discussed. The tapes will only be reviewed by myself and will be transcribed and analyzed. The tape will then be destroyed.

You may feel uncomfortable answering some of the questions. You do not have to answer any questions that you do not wish to. Although you probably may not benefit directly from participating in this study, I hope that others in the community/society in general will benefit by having a better understanding of this critical area of a nurse's world. Your contribution to the body of knowledge is also likely to be appreciated by many.

Participation will be kept as confidential as possible. Study information will be kept in a secure location. The results of the study may be published or presented at professional meetings, but your identity will not be revealed. Participation is anonymous, which means that no one will know what your responses are. For group interviews and focus groups, others in the group will hear what you say, and it is possible that they could tell someone else. Because we will be talking in a group, we cannot promise that what you say will remain completely private, but we will ask that you and all other group members respect the privacy of everyone in the group.

You will receive \$30-\$50 to reimburse you for your time and travel expenses. If you withdraw from the study prior to the conclusion, you will still be reimbursed the same amount. Taking part in the study is your decision. You do not have to be in this study if you do not want to. You may also quit being in the study at any time or decide not to answer any question you are not comfortable answering.

The researcher will be happy to answer any questions you have about the study. You may contact the researcher at 587-377-1927 or send me an email at esackey@shaw.ca if you have study related questions or problems. This research project has been approved on ethical grounds by the University of Saskatchewan Research Ethics Board. Any questions regarding your rights as a participant may be addressed to that committee through the Research Ethics Office ethics.office@usask.ca (306) 966-2975. Out of town participants may call toll free (888) 966-2975.

With kind regards,

Ebenezer Sackey

Phone: 587-377-1927

Email: esackey@shaw.ca

Appendix 3

CONSENT TO PARTICIPATE IN A RESEARCH STUDY

Title of Study: An Exploratory Study of Registered Nurses' Experiences in Patient Information

Supervisor: Arlene Kent-Wilkinson, Department of Nursing, 306-966-6897 (Phone),

Arlene.Kent@usask.ca (Email)

Purpose and Objective of the Study

- The purpose of the study is to gain some understanding of the general experiences of medical-surgical nurses as they relate to patient information privacy and security. The question this study will attempt to answer is what individual nurse experiences are, and how such knowledge could inform further research that will improve policy formulation.

Description of the Study Procedure

- If you agree to be in this study, you will be asked to do the following: Answer a series of questions as part of an interview. You may be asked to elaborate on some of your responses. Upon analysis of your responses, I may ask to speak with you again to seek further clarification. The interview session is designed to take about 30-45 minutes. Location and time of the interview will be primarily decided by the interviewee, at your convenience. With your permission, the interview may be recorded so that I do not miss important components of our conversation. This audio recorded session will later be transcribed onto paper and eventually into a computer for analysis.
- Please feel free to ask any questions regarding the procedures and goals of the study or your role.

Potential Risks

- Breach of confidentiality. Individual interview will only be between the researcher and the interviewee. No other person will be present during the interview. Information disclosed to the researcher during the interview will be kept confidential. If recorded, the media on which it is recorded will be secured in a locked safe and physically destroyed when deemed not needed for the research. Recorded information will be securely kept and remain confidential.
 - If at any point of an interview you do not wish to continue, the interview will be terminated. At that time, if you do not wish for any previous information provided to be included as part of the data, such information will be removed and not included.

Benefits of Being in the Study

- The benefits of being in this study are that you will be contributing to better understanding of the perspectives of nurses in the area of patient information privacy and security. The information you provide will be useful in developing relevant and effective future research and gain a better understanding of how nurses perceive, understand privacy compliance. You will be contributing to the body of knowledge in this area of research.

Confidentiality

- The records of this study will be kept strictly confidential. Research records will be kept in a locked file cabinet and all electronic information will be coded and secured using a password protected file. I will not include any information in any report I may publish that would make it possible to identify you. Information provided will thus remain anonymous. Audio tapes will be stored in locked file cabinets as well. Records will be securely kept for a period of about five years, after which they will be securely destroyed. Paper records will be cross-shredded to ensure that information on them cannot be recovered. Audio tapes will be destroyed by physically breaking them up. This will ensure that information on them are not recoverable.

Compensation

- You will be reimbursed for the cost of transportation to the interview site and back at the end of the interview in the amount between \$30 and \$50.

Rights to Refuse or Withdraw

- The decision to participate in this study is entirely up to you. You may refuse to take part in the study *at any time* without affecting your relationship with the investigator of this study. Your decision will not result in any loss or benefits to which you are otherwise entitled. You have the right not to answer any single question, as well as to withdraw completely from the interview at any point during the process; additionally, you have the right to request that the interviewer not use any of your interview material. Your right to withdraw from the study will apply until data has been pooled together, which is expected to be 3-4 months after this interview. After this period, the information you provided may have been combined with others in ways that may make it almost impossible to withdraw your individual data.

Right to Ask Questions and Report Concerns

- You have the right to ask questions about this research study and to have those questions answered by me before, during or after the research. If you have any further questions about the study, at any time feel free to contact me, Ebenezer Sackey at esackey@shaw.ca or by telephone at 403-986-2628. If you like, a summary of the results of the study will be sent to you.
 - Contact the researcher(s) using the information at the top of page 1;
 - This research project has been approved on ethical grounds by the University of

Saskatchewan Research Ethics Board. Any questions regarding your rights as a participant may be addressed to that committee through the Research Ethics Office ethics.office@usask.ca (306) 966-2975. Out of town participants may call toll free (888) 966-2975.

Consent

- Your signature below indicates that you have decided to volunteer as a research participant for this study, and that you have read and understood the information provided above. You will be given a signed and dated copy of this form to keep, along with any other printed materials deemed necessary by the study investigators.

Subject's Name (print): _____

Subject's Signature: _____ Date: _____

Investigator's Signature: _____ Date: _____

Source of template used: www.smith.edu

Appendix 4

Participant Demographics Form



Demographic Questions

Date: _____ Unique ID: _____

Age:

____ 20-24yrs; ____ 25-29yrs; ____ 30-34yrs; ____ 35-39yrs; ____ 40-44yrs; ____ 45-49yrs;
____ 50-54yrs; ____ 55-59yrs; ____ 60-64yrs; ____ 65-69yrs; ____ Older

Gender: Male _____ Female _____ Other_____

Cultural background: I self-declare as a(an):

- _____ Member of a visible minority
 - _____ Aboriginal person
 - _____ None of the above
 - _____ I choose not to respond

Highest level of education completed:

• _____ Diploma; _____ Baccalaureate; _____ Masters; _____ PhD.

Other Please specify: _____

Job title: _____ Number of years as a registered nurse_____

Full time: _____; Part time _____; Casual _____.

Previous Work History_____

Appendix 5

Interview Guide

Opening Remarks: (Introduce myself)

I would like to thank you for taking time off your busy schedule to talk to me. The purpose of my exploratory research study is to gain insights to what constitutes a nurse's patient information privacy and security experience. The goal is to have a better understanding of this aspect of nursing practice, and to inform future research.

Please be assured that your identity will be protected in regards to information you share with me. Feel free to stop me and ask for clarification at any point in our conversation. If at any time, you would like to terminate our conversation, let me know. Your responses will subsequently be excluded from the data set. It would be appreciated if you could indicate your permission for me to conduct this interview by signing the consent form.

- How has your day been? Busy, I guess. I appreciate the difference nurses make in our society. (Ice-breaker)
- Tell me about what you think patient information privacy and security means in general, and to you personally.
 - Tell me about your experience with patient information privacy and security
 - Probe: Describe for me the things you do that involve patient information
 - Probe: Tell me what you think about patient information privacy regulations that you have to comply with as a nurse?
 - Probe: Tell me what you do when are complying with patient information privacy regulations?
 - Tell me about a situation or situations where you were confronted with patient information privacy issue(s) and how your success or failure in dealing with the situation(s) made you feel about regulatory compliance.
- Tell me about how you acquired your current knowledge and understanding of patient information privacy and security pertinent to nursing practice?
- Tell me about the challenges you face as you carry out your primary duty of caring for patients while ensuring that their information are kept private and secure?

- Probe: Electronic and paper health records
- Tell me about some patient information breaches you have read or heard about that involve nurses and why you think such breaches are occurring.

Closing Questions:

- Do you have any questions for me?
 - Would you like to add anything?
 - How do you feel about this interview?
- Who should I visit with to learn more about my questions?

I would like to thank you again for your time and patience.

(Provide interviewee with my contact information)