Enhancing The Privacy Framework: An analysis of Privacy in Canadian and Brazilian health care

by

Trevor Poole

Submitted in partial fulfillment of the requirements
for the degree of Master of Electronic Commerce

at

Dalhousie University
Halifax, Nova Scotia
December 2014

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

In the last decade, with organizations' increased reliance on digital storage of information, privacy laws have been implemented and updated to help govern the collection, use, disclosure, storage and destruction of personal information. Canada's federal Personal Information Protection and Electronic Information Act (PIPEDA) and provincial acts, like Nova Scotia's Personal Health Information Act (PHIA), have been fundamental in assisting to protect personal information. Emerging countries, like Brazil, are passing laws to protect information due to global economic pressures and hacking breaches to protect citizen's personal information. With a privacy lens, analyzing domestic and foreign privacy laws in conjunction with analysis of a Brazilian neurological center, a supporting privacy framework has been developed. The proposed supporting framework addresses encryption and user roles when accessing information to balance accessibility and usability of personal information.

LIST OF ABBREVIATIONS USED

AES	Advanced Encryption Standard
BRAVA	Brazilian Visual Analytics
DPDC	Department of Consumer Protections and Defence
EHR	Electronic Health Record
EC	European Commission
EU	European Union
ICT	Information and communications technology
MARCO CIVIL	Marco Civil Da Internet
OPC	Office of the Privacy Commissioner
PD	Participatory Design
PHIA	Personal Health Information Act
PIPEDA	Personal Information Protection and Electronic Documents Act
RBAC	Role Based Access Control
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TCD	Task Centered Design
TLS	Transport Layer Security

ACKNOWLEDGEMENTS

First and foremost I would like to thank Dr. Kirstie Hawkey, my supervisor and mentor, for her guidance and direction during this dissertation. Her efforts, in conjunction with Dr. Derek Reilly, provided an opportunity to work with an international research team to complete research within Canada and Brazil. These opportunities helped confirm real-world privacy implementation within a neurological institution in Brazil. I would also like to thank the international research team, which was composed of members from UBC, OCAD University and UFSCar's Advanced Interaction Laboratory.

Without the support and guidance of these people, this dissertation would not exist.

Trevor Poole

Halifax

December 2014

Chapter 1 INTRODUCTION

Within the past 15 years in Canada, the issue of privacy, and particularly digital privacy is one that has become important both socially and politically. In 2001, the Canadian Government passed and implemented the Personal Information Protection and Electronic Documents Act (PIPEDA) to cover the collection, use and disclosure of personal information on the part of government entities and organizations. In 2002, PIPEDA expanded to cover the collection and use of personal information within the "commercial" health care sector, and was applied to all businesses and sectors in 2004 (Levin & Nicholson, 2005).

In 2013, Nova Scotia's Department of Health and Wellness developed the Personal Health Information Act (PHIA) that created additional rules for organizations and professionals that governs how health information is collected, used, disclosed and retained. This balanced approach governs hospitals, nursing homes, pharmacies, physicians and other health care agencies regarding the protection of patient health information in the Province (Government of Nova Scotia, 2014). The government of Nova Scotia implemented PHIA because of concerns that PIPEDA did not do enough to protect patient health information across the full range of commercial companies that collect, use, disclose and store patient data. However, the implementation of PHIA in Nova Scotia actually requires no changes for most health care companies and providers in the Province because, as the government of Nova Scotia has stated, most health care professionals and companies who are in compliance with PIPEDA are already in compliance with PHIA (Government of Nova Scotia, 2013). The importance of PHIA presents in the additional privacy requirements and in the fact it is a provincial act, regarding personal health information. PHIA provides patients more control over the information collected and how the information can be used and was implemented to create a balance between the need

to collect information to help provide care and the right of the individuals to protect their information (DoctorsNS, 2014). Therefore, a physician for instance, has the potential to be charged with both a provincial (PHIA) and federal (PIPEDA) privacy offence. Physicians are now required to report an information breach, if the information loss could cause harm or embarrassment. Under PHIA, there is also a requirement to generate a record of user activity on any health information system where personal health informaton is stored and research now requires the approvial of a research ethics board (DoctorsNS, 2014).

It is the section of PIPEDA that specifically pertains to the health care sector in Canada that has received considerable attention in recent years as the transition away from traditional paper records to Electronic health records (EHR) that can be transmitted over the Internet has occurred (Webster, Ivanova & Cysneiros, 2005). Physicians, hospitals, and health care companies increased their use of EHR within the recent past to more efficiently maintain the health records of patients without the need to maintain large volumes of paper records that are costly to store and easy to lose or damage (Fernandez-Aleman, Senor, Lozoya & Toval, 2013).

With the proliferations of EHR, privacy advocates and politicians raised concerns about privacy issues related to digital records. These are the larger issues of privacy related to the electronic transmission of any information over the Internet (Liu & Park, 2013). The storage and transmission of digital records increases the risk for hackers and others, with the intent to steal personal information, to intercept the EHR of patients. There are a number of articles concerning data being stolen by hackers that are present in the media, as apparent in the theft of a laptop, which contained 620,000 Albertan health care records in 2013. The theft included the loss of names, diagnostic codes and dates of birth (Bennett, 2014). This causes concern about the privacy protections used by health care organizations to protect what is often considered to

be the most confidential of personal information, which is a person's health information (Fernandez-Aleman, Senor, Lozoya & Toval, 2013).

The health care sector is a ubiquitous part of life for Canadians. A single patient of a single physician is not really dealing with only that physician. Instead, the patient directly and indirectly interacts with health insurance providers, government organizations, pharmacies or other organizations that may provide medications, and even other practitioners that work with the physician (Webster, Ivanova & Cysneiros, 2005). In this regard, the issue of digital privacy in the health care setting is an issue that is ever-present in the lives of most people, and certainly most Canadians. A lack of concern regarding digital privacy on the part of any single part of the health care sector could result in having personal health information stolen and potentially misused for harm or embarrassment. Health care custodians that are capturing personal health information need to be educated on the issues regarding privacy in both the context of PHIA and PIPEDA. As an agent or custodian of personal health information the issues surrounding privacy cannot be avoided by choosing one type of health care provider over another, or deciding not to do business with one company in favor of another. Instead, as paper records are migrated to EHR and breaches of information from hackers becomes more of a reality, protecting information becomes more critical. The use of EHR by health care providers now includes everything from direct patient records to billing to filling prescriptions (Webster, Ivanova & Cysneiros, 2005).

1.1 Themes and Concepts

Several underlying themes and concepts must be recognized as important as we examine the issue of digital privacy in the ubiquitous health care setting. It is not simply a matter of privacy laws or health care providers being limited in the information they can collect and share

with others. Instead, digital privacy involves a range of themes and concepts from 1) the legal requirements dictating privacy 2) to the larger marketplace in which health care providers operate, to 3) the technology that makes it possible for EHR to exist at all. In addition to these three themes, Canada has been the focus of criticism because of the fact that the burden of identifying breaches in privacy rests largely with citizens and not with the companies that collect and share personal information (Bailey & Caidi, 2005). Within Nova Scotia, the collection of personal health information in conjunction with PHIA has shifted the responsibility to the custodian or agent of the EHR. With the expansion of EHR systems and the desire of health care providers and patients to be able to easily access records over the Internet, the issue of how to enhance privacy is one that is only likely to become an even greater concern. At the same time, the issue of enhancing digital privacy is not just an issue for Canadians, but an issue for individuals around the world (Fernandez-Aleman, Senor, Lozoya & Toval, 2013).

In Canada, the first theme related to digital privacy in health care is the implementation of privacy laws that dictate digital privacy. The Canadian Constitution does not provide a specific right to privacy (Levin & Nicholson, 2005). The Personal Information Protection and Electronic Documents Act was established in order to provide privacy protections to citizens and business, while conducting commercial activity, when collecting, using and storing personal information. (Lasprogata, King & Pillay, 2004). To enhance the privacy of personal health information, PHIA in Nova Scotia was introduced in 2013, which bears similarity to PHIA in Newfoundland, Manitoba and other health information privacy acts within the provinces of Canada.

Interestingly, PIPEDA does not place the entire burden on the companies to report breaches when collecting personal information. Instead, while PIPEDA sets standards (e.g.,

companies should only collect the information that they need and should maintain the accuracy and privacy of that information), it is the responsibility of citizens and ethical businesses practices to file incident breaches, if a situation has been identified where the collection, use or disclosure of personal information has been violated (Bailey & Caidi, 2005). It is in the interest of the business to ensure privacy, as it is a part of the customer experience that can promote a level of trust to between the customer and the business. Privacy breaches are filed through the Office of the Privacy Commissioner (OPC) and in rare instances a privacy incident breach can be opened by the OPC, if the breach is of a serious nature (Office of the Privacy Commissioner of Canada, 2008). Personal information privacy in Canada, including patient information, does not involve strict requirements of health care providers to report violations of digital privacy under the provisions of PIPEDA. Health information acts, like PHIA in Nova Scotia, have reporting requirements: "PHIA requires that a custodian must report a breach of personal health information to an individual if, in the custodian's opinion, the breach is likely to cause the individual harm or embarrassment" (Government of Nova Scotia, 2013).

The second theme involves the health care market and how health care is able to function as a sustainable model for long-term investment by organizations. Government legislation, regarding privacy laws, is not simply about the needs or concerns of citizens, but also about the abilities of companies to operate and compete against each other in a balanced marketplace (Bailey & Caidi, 2005). Establishing very strict privacy rules for companies might be desired by citizens, but would be counter intuitive for organizations, such as health care providers, who would be unable to provide the most efficient or effective services. In this regard, government regulators must balance privacy legislation with the needs of the larger marketplace.

The third theme involves the use of Electronic Health Records (EHR) and takes into consideration the technology to storage of electronic files with patient information on remote servers. EHR have become so widely used and desirable as a means of maintaining patient information because of the ease of access in sharing information across the Internet with other health care providers (Liu & Park, 2013). The ability to maintain and share large amounts of patient data requires the use of servers that are often maintained by third-party organizations. The businesses that maintain the digital records must have technologies in place that allow for the storage and retrieval of information and, also the protection of data while in transit across the Internet (Fernandez-Aleman, Senor, Lozoya & Toval, 2013).

The concept of cloud computing, or the storage and access to information and applications over the Internet, has become critical; it can present opportunities to reduce the cost of information storage however, the increased risk of data breaches exists. Hackers have become a threat by gaining access to those servers or by intercepting records as they are transmitted with the result of information being captured for personal gain (Fernandez-Aleman, Senor, Lozoya & Toval, 2013). Digital security and the security framework that health care providers and health care companies use to protect personal health information that is stored in the cloud is an industry to itself. However, it is physical and non-physical security that directly impacts the privacy of patient information and whether patients are at risk of having their personal health information stolen. It is possible that efforts to improve digital privacy in Canada can serve as a model for greater digital privacy in emerging nations in which health care systems are expanding to include more individuals. The lessons learned in countries that have more developed privacy laws, such as Canada, can enhance digital privacy for emerging nations until such time as those privacy laws develop and therefore normalize the protection of personal information.

1.2 Aims and Objectives

The main aim of this research is to propose a supporting privacy framework to enhance existing digital privacy frameworks in health care. The supporting framework will present privacy and security elements that can be adapted to the health care systems in Canada and emerging nations like Brazil. This is completed though researching the privacy issues and concerns that are currently part of the health care system in Canada and Brazil. A supporting goal of this research is to understand the ubiquitous technology that is part of the process of digitally capturing, storing, and sharing patient information. Research that was captured and analyzed during a workshop in Brazil and research that was previously completed by peers within the same Brazilian hospital provided the data necessary to assist in constructing the main research objective of creating a supporting privacy framework.

1.3 Research Process

A novel opportunity to join an ongoing research project, entitled BRAVA, presented itself during this research process. BRAVA was investigating emerging technology in the country of Brazil. The initial focus of the BRAVA project was on mobile visual analytics for health care and medical applications. The research team was a collaborative effort between Dalhousie University, University of British Columbia, OCAD University and UFScar's Advanced Interaction Laboratory located in Brazil. My role, once I collaborated with BRAVA, was to analyze workshop data collected within the Brazilian hospital, review two published research papers about the Brazilian hospital, and research privacy law in Canada and Brazil. My goal was to construct a supporting privacy framework that could enhance existing health care frameworks within Canada and emerging counties.

Prior to the BRAVA project, the Brazilian facility was primarily using pen and paper practices to collect, use, disclose and store personal health information, making the implementation of technology within the health care facility a novel concept for its health care professionals.

The first step of the research process was the literature review, which consisted of privacy background information and an analysis of privacy legislation in Brazil. I also took part in a site visit to a Brazilian hospital to help facilitate a workshop. In addition, I reviewed the project's prior published and non-published research from the same hospital in Brazil, using a privacy lens on their findings. During the three-day workshop, staff were introduced to a tablet environment and taught the basics of tablet use, which included how to take notes, make videos, take photos, capture voice recordings and use pre-installed software. The purpose of the workshop was not only to introduce the basic use of tablets, applications and prototypes, but also to capture the person-to-technology interactions, so that I could later construct a supporting privacy framework within the body of this thesis. Researching both Brazilian and Canadian privacy legislation was important because it provided an opportunity to build a supporting privacy framework though the understanding of an emerging country's tension between privacy and technology adoption, as is occurring in Brazil, in contrast with Canada's more developed privacy act and technology platform.

1.4 Structure of the Thesis

Chapter 1 presents themes and concepts, aims and objectives and the research process fpr the thesis. Chapter 2 provides a basic background and overview of the issue of digital privacy in the health care sector in Canada. Chapter 3 provides a privacy analysis of Brazil legislation, including how privacy in Brazil compares to privacy in Canada. Chapter 4 presents a workshop

and case study of a Brazilian hospital and the digital privacy issues that are present within that hospital. Chapter 5 provides a privacy framework for improving digital privacy in Canada and includes a discussion of how adaptations of the recommendations that are provided can be implemented in Brazil. Finally, chapter 6 concludes with recommendations for future work on this subject.

Chapter 2 BACKGROUND AND RELATED WORK

2.1 Introduction

This chapter provides a literature review related to the three major themes and concepts that have been identified as important in the examination of the enhancement of digital privacy within a ubiquitous health care setting: 1) the legal requirements dictating privacy; 2) to the larger marketplace in which health care providers operate, and 3) the technology that makes it possible for EHR to exist in their current form. For each of these themes, a review of recent literature will be provided in a critical manner; therefore the information from various studies will not simply be presented. Instead, a critical analysis of the information and ideas that are presented will be provided.

The information presented in this chapter will serve as a background for a case study and workshop, as well as the creation of a supporting privacy framework. The literature that was reviewed will be analyzed in a critical manner in order to determine areas in which conflicting findings or ideas are present. Moreover, the literature needs to be reviewed in such a way as to allow for the best opportunity to analyze issues related to EHR and digital technology to create linkages with privacy legislation in Canada. In this regard, I begin with a review of information about EHR (2.2), followed by a review of cloud computing (2.3). In section 2.4, a review of the digital technology that is used in the medical environment is provided. Next, the review shifts to patient privacy, with a critical analysis of privacy rules that are related to medical practices and medical companies in Canada (2.5).

2.2 Electronic Health care Records

EHR are what the name would imply: computerized patient records that are collected, stored, and retrieved using information management systems specifically designed for use by medical organizations, medial providers, and patients (Boonstra & Broekhuis, 2010). Over the past decade, a major push has occurred in Canada, the United States, and other countries around the world for physicians, hospitals, and other medical providers to move away from traditional paper records to electronic records as a means of allowing for greater sharing of patient data in a more efficient manner (Ball, Smith & Bakalar, 2007). One of the reasons that the concept of EHR has been embraced by many medical providers and by governments is that the use of traditional paper records not only requires a great deal of space, but makes the efficient exchange of information for the sake of providing a continuity of care for patients very difficult (Boonstra & Broekhuis, 2010). It is very easy for paper medical records to be lost or misplaced. At the same time, it can be difficult to find the specific information that another physician or medical provider needs for patients with large medical records.

The argument has been made that paper records provide some benefits over EHR, such as the ability to be flexible in terms of the information that is collected; they are not realistic in present day in which computerized support and computerized processing of information is necessary (Wollersheim, Sari & Rahayu, 2009). EHR are often very rigid with regards to the type of information that medical providers must collect or the way in which medical information about a patient must be collected. The format of electronic records maybe standardized so that they can be used to collect information for different patient triage scenarios to cope with different situations. The electronic nature of the health records also means that rather than sending paper files through the mail or a delivery service, which can still require days for health

records to be transported from one location to another, medical records can be shared electronically almost instantly (Boonstra & Broekhuis, 2010). Fax also represents another method of transmitting information, although speedy, there are issues regarding sending to a shared office environment.

On the surface, it would seem that the move from traditional paper medical records to EHR should be without controversy. Medical providers are able to more easily and efficient access patient records, and patients are able to receive information, medical advice, and medical services faster and more efficiently. At the same time, because of the increased efficiency and lack of needing to deal with paper records, research has shown that medical providers can actually see a positive return on the initial investment of information systems and digital devices for the use of electronic medical records in only 2.5 years (Miller, West, Brown, Sim & Ganchoff, 2005). However, concerns about interoperability of EHR systems and patient privacy have been raised.

With regards to interoperability of medical record systems, there are a variety of information systems that are available for physicians, medical providers, and other medical-related companies to obtain and store patient data (Wollersheim, Sari & Rahayu, 2009). Differences in EHR systems can create incompatibilities; therefore the ability to share medical information would not take place.

There is an effort to create international standards for electronic record systems to deal with the problem of interoperability (Wollersheim, Sari & Rahayu, 2009). The enforcement of international EHR system standards would still allow different companies to create and market their own EHR systems. However, the presence of the standards would mean that a similar format for the actual patient records would exist so that medical providers would be assured that

the systems they purchase would be able to read the records created and used by providers with competing systems.

Concerns have been raised by both the general public and politicians about the safety and security of the patient data that is collected, stored, and shared over the Internet (Angst & Agarwal, 2009). The electronic coding and sharing of patient data over the Internet between providers and even among individual providers, raises the concern that hackers and others might be able to access the data and cause harm to patients (Kalra, 2006). Patient medical records are considered to be some of the most important and most confidential of information that exists about any particular individual (Fernandez-Aleman, Senor, Lozoya & Toval, 2013). A person or group of people who want to gain financial benefits, such as stealing identities or using personal information in some other way, would easily be able to do so by gaining access to personal medical records.

In order to protect the privacy of patients, governments such as Canada and the United States have implemented various rules and laws that dictate how patient medical records may be collected, stored, and used (Angst & Agarwal, 2009; Levin & Nicholson, 2005). The goal of these laws is indeed to protect the privacy of patients and to place responsibilities on medical providers to collect and use only the information that they need in ways that will protect that information. This certainly seems important given that a person's medical information may be given to a physician who then has to share it with an insurance company, pharmacy, and even other medical professionals in the same practice in order to provide the full range of medical care that is needed.

However, the issue of patient privacy and the protection of EHR should not be viewed as a reason to avoid using electronic systems for the collection, storage, and retrieval of patient

information. In fact, politicians have noted that patients actually do want to have easy access to their medical records (Angst & Agarwal, 2009). The days of paper medical records made it very difficult for patients to be able to easily access their own records, and certainly made it difficult for both patients and providers to share those records in order to achieve a high continuity of care. Electronic medical records provide a benefit for patients in terms of being able to access their own records, as well as know that their records are being shared with a reduced threat of records being lost or damaged in some way.

In fact, some hospitals and medical providers are now making it easy for patients to access their medical records by providing online access to those records (Angst & Agarwal, 2009). This is important because for the first time, patients can have real-time access to their medical records to allow them to make decisions about their own health needs and issues (Ball, Smith & Bakalar, 2007). At the same time, this is also a way for medical providers to demonstrate a personal usefulness for EHR to patients. Once patients have the ability to access their medical records over the Internet, it would seem unlikely that they would want this ability to go away. However, this does not mitigate the issue of privacy protection. If anything, the increased demand for patients to be able to take full advantage of EHR would seem to increase the importance of enhancing digital privacy in the health care setting.

2.3 Cloud Computing

As defined by the National Institute of Standards and Technology (NIST), cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NSIT, 2011). The definition may seem

ambiguous in nature, but it reflects different service models, storage options, software packages and overall architecture. Cloud computing operates by providing a remote Internet access to a where desktop, laptop and other mobile devices might be used to collect, use, disclose and store information. A health care provider, for instance, could collect data from patients at one location and have that information readily available by a second office. This could take the form of the collection and disclosure of an X-ray, where the information could be shared with the patient and doctor from the same cloud computing data storage. Through the use of a cloud computing service, the health care provider could store all data remotely, not have local storage and and retrieve information as it is needed (Rolim, Koch, Westphall, Werner, Fracalossi & Salvador, 2010).

Cloud computing architecture is attractive because the costs and effort of maintaining information technology can be outsourced to another organization. Within the IT industry, the concept of Software as a Service (SaaS) has arisen in which third-party companies provide computing services to companies in which they maintain the applications and the storage devices on which those applications and the related data that are collected and used are maintained (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, patterson, Rabkin, Stoica & Zaharia, 2009). One company that is well known for providing cloud-computing services to all types of companies is Amazon through its Amazon S3 cloud service (Doukas, Pliakas & Maglogiannis, 2010). Amazon provides companies with access to web interfaces on which various applications, often database applications, are used to collect, store, and share information.

Cloud computing is not the only option that is available, but it does offer the most flexibility for information access. For instance, a physician's office could have an intranet and closed network which would provide the most security, but would lack the data sharing

capabilities could provide a faster health care experience if the patient needed their records at a remote location. Cloud computing has become popular within the health care industry because of the costs incurred by health care providers to operate and maintain a variety of applications along with the server space. In addition, there are also considerations for maintaining the server architecture and by using an outsourcing model to manage the costs of costly server upgrades and maintenance fees (Padhy, Patra & Sataphathy, 2012). Organizations within the health care industry, whether they are private practices or large companies that provide prescriptions, utilize many applications and can have the capacity to store large amounts of data. However, by using a cloud computing service, a health care company can place the burden of maintaining software and hardware on a third party (Doukas, Pliakas & Maglogiannis, 2010).

For example, a small medical practice that operated its own software and hardware might project that it will need a specific amount of space to store the electronic files of its patients for the next five years in conjunction with an IT resource to manage the solution. However, after only three years, the practice might find that it needs more storage space. If this were to occur, then the medical practice would have to incur the costs of buying additional servers to handle its storage needs. With a cloud computing service, additional storage space is always available. The medical practice might be charged more per month for the service based on the amount of additional storage space needed, but this cost would be far less than the cost to purchase and install its own servers (Rolim, Koch, Westphall, Werner, Fracalossi & Salvador, 2010).

From a broad perspective, the primary advantage of cloud computing with regards to finances is that a medical practice only has to incur a monthly fee to have the computing and storage power that is needed (Padhy, Patra & Sataphathy, 2012). The upfront cost of purchasing large IT systems is gone. In addition, most cloud computing services update the software that is

being used on a regular basis, as well as the hardware on which the software is run (Rolim, Koch, Westphall, Werner, Fracalossi & Salvador, 2010). A medical practice or hospital can be assured that it will be using the latest patched software on the latest hardware at all times. All of this can occur with a monthly fee rather than large initial capital outlays followed by large costs to maintain and upgrade systems on a regular basis.

Aside from the issue of cost with regards to the use of cloud computing in the health care industry, another advantage of cloud computing in medicine is the remote aspect of using multiple devices for data collection, use and retrieval (Doukas, Pliakas & Maglogiannis, 2010). Physicians and other personnel in a medical practice or hospital are not tied to a desktop computer or even a laptop computer, where the information can be stored remotely. Instead, they can assess the data they need and keep the data from residing on a device that could be lost or stolen. The limitation for this type of access would be a server failure, poor Internet connectivity or user issues like lost usernames and passwords..

While the information provided thus far about cloud computing might make the idea of cloud computing and Software as a Service seem to be without problems, but there are major issues that must be considered. The idea of storing data on remote servers and retrieving it entirely over the Internet raises the issue that the data could be intercepted by hackers or that databases could be accessed by password theft or brute force attacks (Nkosi & Mekuria, 2010). In this regard, several layers of security must be used to protect data located on remote servers. The most basic form of security is authentication security, whereby a user must provide login, password or other identifying information in order to be able to access remote data (Padhy, Patra & Sataphathy, 2012). Authentication can take many forms, where companies like Google and Samsung are interested in making passwords obsolete. Fast identity online (FIDO) is a new

technology that uses hardware, like a USB key, or biometric data to authenticate users (Sparks, 2014). The authentication information of users must not only be encrypted, but users should be required to change password or pin information on a regular basis in order to mitigate the potential for brute force, hack or stolen access information. At the same time, even as the data is sent over the Internet, encryption must be used so that hackers cannot intercept the data being sent and easily decipher it for personal gain (Nkosi & Mekuria, 2010). The use of various types of encryption can protect the data that is transmitted, so that others are not able to read the data.

There is also the consideration for privacy law, where acts like Nova Scotia's Personal Health Information Act (PHIA) state that storing personal health information outside of Canada is prohibited unless "the head of a public body, or the responsible officer of a municipality, determines that it "meets the necessary requirements" of the organizations operation" (Government of Nova Scotia, 2013). If there is a decision to store information outside of Canada the process also includes notifying the Minister of Justice and provide details as to why the decision to store information in a foreign country..

Time also presents challenges, as health care workers would need to invest time researching what security procedures cloud computing services use, as well as auditing those procedures to ensure that personal health information is protected (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica & Zaharia, 2009). The challenge of time or not understanding the technology would be magnified the smaller the practice, where there would be very limited resources, but this is not unique to cloud computing and is more of an ubiquitous issue.. The leaders of medical practices, hospitals, and other health care providers cannot simply remove themselves from the issue of data security because they use a third party cloud computing service. Instead, health care practices and providers must be a part of the

review to understand the fundamental security procedures and the security lapses of the cloud computing services they use. As well, the health care provider should understand if the cloud computing service is compliant with local privacy laws where the provider is operating. Research is important to help ensure that the security procedures for cloud computing that is selected are appropriate; otherwise security procedures of other cloud computing services need to be reviewed so that a change in the service that is used can be made.

Cloud computing can be an important part of the implementation of EHR. As compared to other options, such as purchasing and maintaining internal servers, cloud-computing can reduce IT costs for health care providers, so that the most efficient IT services can be used. Paying for the space and services you need today, with provisions to grow can reduce costs, and avoid costly infrastructure upgrades in the future. Purchasing and maintaining internal servers and paying for IT support can be much more costly than using a third-party provider that can handle both the storage services and the IT maintenance services (Padhy, Patra & Sataphathy, 2012). However, the issue of security cannot be ignored because another company is maintaining the IT systems the health care provider is using. Instead, medical practices and medical providers have to make personal health information security part of how they operate regardless of whether the data are actually stored. This requires a combination of efforts in terms of interactions with the cloud computing company and in terms of educating employees (Nkosi & Mekuria, 2010). Educating employees is just as important as any encryption standard implemented on a system, where employees can present their own security threat. Information on social engineering, authentication options like retinal or thumbprint, key cards and digital security keys is also another important measure that must be taken, so employees do not take actions that might compromise the security of cloud computing systems, so that personal health

information is protected. The key is for medical practices to understand both the benefits of cloud computing, as well as the potential problems that can occur with regards to data security and privacy.

2.4 Digital Technology

Data Collection. One element of EHR and electronic data that was briefly mentioned in the discussion of cloud computing was the use of tablets and smartphones as a means of collecting and accessing patient data. While the inclusion of tablet, smartphones, and other portable devices in any discussion involving technology in the present era may seem normal and not extraordinary, some discussion and considerations about the use of tablets and other smart devices with regards to patient data is necessary. Handheld devices have actually been used in medicine in some form for nearly two decades (Embi, 2001). The release of some of the first handheld devices occurred in the early 1990s, which brought about the ability of people to collect information and store files without being constantly connected to a larger desktop computer (Fischer, Stewart, Mehta, Wax & Lapinsky, 2003). The problem, however, with the early handheld devices was that they were not strong in terms of their computing power, and often lacked the ability to wirelessly connect to other computers (Embi, 2001). In this regard, data that were collected on the devices had to be downloaded to a larger computer by connecting the device to the computer with a wire.

However, with the proliferation of better cellular data networks and Wi-Fi Internet connections in offices, handheld devices have not only grown in usage in all aspects of society, but in medicine (West, 2012). In fact, it has become quite common in hospitals and medical practices to witness physicians, nurses, and other professionals carrying tablets and other smart devices on which they are collecting, using and disclosing patient data (Bolton, Gassert &

Cipriano, 2008). The reason for this is that smart devices are easily appropriated to take photo's, communicate with peers, analyze information and makes it possible for medical professionals to collect and share data from nearly any location provided there is an Intranet or Internet connection (West, 2012). In previous decades, physicians, nurses, and other medical professionals were essentially tied to desktop computers and pen and paper practices. Information and patient data was often written on paper and then inputted into computers by somebody else at a later time. If information was needed immediately, the time and effort had to be taken to find a desktop computer to use, which might have meant leaving the patient while retrieving the information.

With the proliferation of handheld technology and wireless Internet services, it is possible for medical professionals to collect and retrieve patient data while standing in front of the patients (Varshney, 2007). Embedded medical devices that are present in patient rooms, like heart and blood pressure monitors could also offer additional information to assist physicians in retrieving real-time information, as well as input storage into electronic health files.. The real benefit for both physicians and patients is the ability to review the full range of data that are available about a patient without having to wait. The combination of EHR and handheld device usage in hospitals and medical practices means that all of the available data about a patient can easily available for the purpose of making decisions about future care.

Efficiency. Furthermore, from a standpoint of efficiency, the use of tablets and other smart devices allows for medical care to be provided in a cost efficient and efficient manner. (Lapinsky, Weshler, Mehta, Varkul Hallett & Stewart, 2001). All of the medical professionals in a practice or hospital can be equipped with smart devices for a relatively low cost per unit. However, for this cost, the medical professionals can input data in real-time, which eliminates

the need for another person to enter data from paper records that might get lost or damaged. In addition, if the larger interest in electronic medical records is about being able to share patient data with other medical providers, then the data need to be as up to date as possible at any given time. By inputting data into patient records in real-time with electronic devices, the data can be shared in real-time with the knowledge that it is up to date as possible.

The use of tablets and smart devices would also seem to make sense if the goal is to move away from paper records and use EHR. It does not seem appropriate to want patient records to be in electronic format only to initially collect the data using paper when it can be avoided. In this regard, the use of tablets and other handheld devices is not only about reducing costs, but is also about being as efficient as possible in providing health care services and collecting and using patient data. This is very important in situations in which immediate decisions have to be made, such as in intensive care units (Lapinsky, Weshler, Mehta, Varkul Hallett & Stewart, 2001).

Remote Monitoring. Smart devices are being used on a larger scale to automatically collect data from patients when they are away from medical providers (Varshney, 2007). The use of remote sensors that are connected to patients are in use as a means of monitoring the health conditions of patients with certain illnesses, such as high blood pressure or histories of heart attack (West, 2012). The devices are worn by the patients and collect data on a regular basis, such as every three hours or every six hours. Therefore, the personal health information would automatically be sent to their personal heath record, so their physicians or other medical provider could review the collected data. Devices like Fitbit, Microsoft band, smart watches and other fitness trackers that are collecting information could be setup to provide real-time information to your EMR and access by your physician.

For people in live in rural areas, the use of smart devices on the part of medical professionals means that it is possible to receive the same level of care and support as patients who live in urban areas that are able to visit a physician's office (Varshney, 2007). A physician with patients in rural areas can visit those patients, and through the use of cloud computing technologies, can access patient data and other records from that rural location. There is no need to bring along large paper records because of the inability to access the electronic records that are available in the office.

In turn, the ability to have the complete electronic records of patient at hand in nearly any location also reduces the potential for errors to be made because of a lack of information (Varshney, 2007). On a broad level, the idea of reducing medical errors that are made simply because of not having the complete medical information of a patient is certainly an advantage of the proliferation of digital technologies in medicine. However, the changing nature of the population, particularly the increase in the older population and the increase in acute care needs, means that reducing medical errors and being able to make on the spot decisions is more important than ever (Bolton, Gassert & Cipriano, 2008).

One of the benefits of what is known as pervasive health care, meaning health care at any time and in any location, is the ability to help patients monitor chronic illnesses, while also being able to immediate notify medical personnel in the event that vital signs indicate that immediate treatment is needed (Varshney, 2007). At the present time, there is a push within the health care industry to reduce costs by focusing on preventative care (West, 2012). The use of smart devices to constantly monitor patient conditions is a means of reducing costs by using patient data to prevent major problems from arising. For example, rather than a patient with a history of heart attacks only being treated when another heart attack occurs, a sudden change in blood pressure,

breathing, or other vital signs could be used to alert a patient and his or her physician that some type of intervention is needed to prevent another heart attack.

The proliferation of faster and better wireless Internet services has meant that medical professionals can utilize smart devices from almost any location to access patient data (West, 2012). The personal monitoring of patient conditions with sensors that can collect and send data to medical professionals, and alert patients to changes in their health conditions in real-time, really is an extension of the use of the Internet and cloud computing to provide health care services. Patients can essentially collect their own personal health information, but it is important to remember that under acts like PHIA, the information would not be protected unless it was collected, used or disclosed by a heath care organization. Sharing the information with your doctor would subject the information to PHIA. This would true as well for PIPEDA, where the data would not be protected unless under commercial activities, there in lye's the risk of collecting personal information and privacy legislation.

One other issue that has not been raised is the issue of security for the use of tablets, smart devices, and sensors that collect, use and disclose information about patients in real-time. The use of smart devices and sensors is really an extension of the cloud-computing infrastructure, if the information is stored remotely over the Internet. If the information is stored locally and captured by a local device, then risks like physical removal of the senor and therefore data and local hacks are risks. In this regard, the same security issues for protecting personal health information and privacy exist with those devices on a cloud network or local storage exist Even with the best electronic security, physical security must also be maintained to ensure that devices are not stolen or used by those who have no need to access patient information (Cucoranu, Parwani, West, RomeroLauro, Nauman, Carter, Balis, Tuthill & Pantanowitz, 2013).

The underlying issue of concern is ensuring that patient privacy is protected, as well as ways in which to enhance that privacy as EHR and the electronic collection of all types of patient data expands in Canada and around the world.

The importance of the information that has been examined with regards to digital technologies in the collection and retrieval of patient data is the recognition that EHR are about more than data collected in a physicians office and shared with hospitals, and possibly insurance companies. EHR are also about data that patients might collect themselves with the use of monitors and sensors. This poses a number of risks that would include data integrity, security and management of the information. In this regard, EHR become a greater part of the lives of nearly everybody in the country. Patient data can be collected, stored, and retrieved in traditional medical facilities, in rural areas with a tablet or smartphone, or sent to a hospital or other medical provider from a small sensor.

2.5 Patient Privacy

Patient Privacy. The final issue to be discussed in this chapter, and the issue that might seem the most important and relevant to this research, is patient privacy. Specifically, the focus of this section of the review will be about the legal framework for patient privacy in Canada, as well as the responsibilities of both medical providers and patients in fulfilling that legal framework. The basis for patient privacy in Canada is the Personal Information Protection and Electronic Document Act (PIPEDA) (Samsuri, Ahmad & Ismail, 2011). PIPEDA was not specifically created for the purpose of patient privacy when the legislation was passed in 2001 and has limits on commercial activity only. Instead, the Act was initially implemented as a means to place limits and controls on private-sector organizations and how information is collected, used and disclosed PIPEDA was expanded in 2002 to apply to the collection of

personal information within the health care sector, and was further expanded in 2004 to cover the collection of personal information by all businesses, both public and private (Levin & Nicholson, 2005).

Acts such as PIPEDA are not unique to Canada. In the United States, and other parts of the world, laws and regulations have been implemented within the past decade with a focus on increasing the privacy and protection of patient information and data (Scott, Jennett & Yeo, 2004). These laws have been written with a focus on the type of data that are collected, how the data are used, and how the data are shared with other companies and entities (Win, 2005). In this way, Canada is not necessarily ahead of other developed nations with regards to efforts to protect patient privacy. At the same time, Canada is not behind other countries. Instead, the effort over the past decade to increase privacy protections related to patient data is a trend that has occurred in many developed nations.

The limit of protecting privacy has not ended with the federal legislation of PIPEDA. On December 2012, the provincial Personal Health Information Act (PHIA) was proclaimed in Nova Scotia, and came into force on June 2013. As with PIPEDA, the implementation of the provincial PHIA was designed to balance the concern of patient privacy and the protection of patient data with the need for medical providers and third parties to share patient information in order to provide care and other services. The act not only recognizes the right of the individual and the protection of their EHR, but also defines the requirements of custodians to manage and support health care when information is collected, used or disclosed (Government of Nova Scotia, 2013). Even though PHIA has provisions to force agents and custodians to disclose when breaches of information occur, it is limited to health care. This is an important consideration,

where if an individual or organization collects, uses or discloses personal health information that was not collected for the purpose of health care related activities PHIA will not be applicable.

Defining Personal Health Information under PHIA. There are four important means of identifying if information is about an individual. If the information describes the physical or mental health of the individual, relates to the history of the individuals family, describes the provision of health care to the individual or devolves information of payments or eligibility for health care in regard to the individual (Government of Nova Scotia, 2013).

Defining Personal Information under PIPEDA. "In the health context, personal information means information about an identifiable patient which includes any factual or subjective information, recorded or not, about that individual, including health related information." (Industry Canada, 2013). The first issue that would seem to be of importance is the requirement within PIPEDA of the protection for personal information (Schwartz & Solove, 2011). The idea of personal information might seem like a simple concept, but there are complexities. People might consider information about themselves such as names, addresses, and even their ages to be personal information.. However, the definition of personal information that is contained within PIPEDA is identifiable information, meaning information that allows for someone else to specifically identify a particular individual (Adams, 2006). Some information might be personal, such as the blood type of a person, but it may not be information for an identifiable person. The question might be asked as to whether a person's blood type, for example, would really allow for a total stranger to identify a specific person.

This issue of personal information as compared to identifiable information should immediately raise questions about the specific type of information that is protected under PIPEDA. While people might view almost any information about themselves to be personal, it is

the information that makes it possible for a stranger to identify a person during a commercial activity that would be protected under PIPEDA. A growing concern is the ease of accessing combinations of information that can then be integrated and used to identify individual patients. Questions can be raised as to how specific information must be categorized and integrated before it actually allows for someone to be identified. In real-world practice, is it possible to identify a person simply based on height, blood type, or even hair color? This question of what exactly constitutes identifiable information under the definition of personal information has been the basis by some to argue that patient protections under PIPEDA are not strong enough (Adams, 2006).

The issue of what constitutes personal information as compared to identifiable information might appear to be only of concern for lawyers or those with an interest in the law. However, the idea of personally identifiable information is the basis for PIPEDA, which means that it is the basis for the responsibilities of companies and entities to protect patient data (Schwartz & Solove, 2011). If the data collected about patients are not considered to allow for personal identification, then those data are not protected under PIPEDA, meaning that entities have no responsibility to protect the data. A medical practice might collect information about a patient, but the information that was collected, used or disclosed might not be considered to be personally identifiable and if there is no commercial activity, it would not subject to PIPEDA.

As the above discussion demonstrated there is a basis for concern about patient privacy in Canada and a discussion and study of ways to enhance digital privacy is necessary. The protections that citizens might believe are present within the legal framework may not be present at all. At the same time, the legal intricacies of the definition of personal information could create a situation in which information about a person can be shared because there was no

commercial activity or does not have to be protected because it cannot be used to actually identify someone. There should be some confidence in the system, as doctors and other medical providers operate under a code of ethics that would offer its own layer of privacy protection.

Provider and Patient Responsibilities. I next examine the issue of the responsibilities of both medical providers and medical companies, as well as the responsibilities of patients under PIPEDA and PHIA. Medical providers and organizations are required to obtain consent from patients when personal information is collected. The personal consent must contain information about how the personal information will be used, as for what reasons it would be shared with other entities (Kerr & Caulfield, 2008). In addition, medical providers face guidelines about how they are to handle and protect patient data (Peyton, Hu, Doshi & Seguin, 2007). Under PIPEDA, the collection, use and disclosure of personal information is governed only during the course of commercial activity. PIPEDA is a federal act and therefore has no bearing on publically funded hospitals (Government of Nova Scotia, 2013).

In addition, medical providers under PIPEDA are required to ensure that when they provide patient information to third parties, those third parties are only using it for its intended purpose (Kosseim & El Emam, 2009). For example, a physician is likely to provide patient information to a pharmacy that is necessary for a prescription to be filled. The responsibility of the physician is to only provide the information that the pharmacy needs to fill the prescription. In addition, the pharmacist is then responsible for ensuring that the pharmacy will protect the information that it is provided and not use that information for other purposes. The responsibility of the initial entity that collected and shared a patient's personal information does not end once the information has been provided to a third-party. While the third-party has its own responsibilities under PIPEDA, the initial party that collected the information continues to

be responsible. The physician cannot argue that he or she was unaware that the pharmacy was misusing patient information.

PHIA has a much more inclusive definition of what is protected, which extends to include personal health information that individuals or organizations are in control of, as defined by the act. PHIA also governs the collection, use and disclosure and has provisions for the retention, disposal and destruction of personal health information (Government of Nova Scotia, 2013).

As part of the patient protection requirements of PIPEDA, physicians and medical providers that collect information must also have a process for patients to submit complaints and inquiries when they believe that their information has not been fully protected or has been misused in some way (Nisker, 2006). For example, if a patient believes that his or her personal health information that was provided to a physician has been obtained by a third party that should not have that information, then a complaint can be filed with the physician and the complaint must be investigated. The requirement to investigate complaints or concerns that patient data have not been fully protected or have been misused in some way would seem to be a standard part of protecting patient data. However, the full responsibility of patients to initiate investigations of the misused or lack of protection of their data may not be fully understood by the public.

While PIPEDA requires that medical providers and third parties protect patient data and prevent that data from being stolen or misused, those providers and third parties are actually not responsible for reporting the theft or misuse of data. Instead, it is the responsibility of patients to report and initiate investigations of stolen or misused data (Bailey & Caidi, 2005). If a patient has identified a situation in which his or her personal information has been misused, then it is his

or her responsibility to file the complaint so that an investigation can begin. It is not the responsibility of a medical provider or third party to begin an investigation on his or her own.

In summary, a key issue to understand is that personal health information in Canada is not something that is the sole responsibility of medical providers and third parties (Bailey & Caidi, 2005). PIPEDA was written in a way that places certain responsibilities on medical providers and third parties, but also places certain responsibilities on patients (Nisker, 2006). Medical providers must protect patient data and only collect the data that they need. At the same time, medical providers cannot share personal information with a third party unless there is a need for that information to be shared. However, patients have the responsibility of discovering if their personal information has been misused or not fully protected. Then, they must file a complaint with the responsibility medical provider or company that collected the information so that an investigation can begin.

The concern that exists with the way in which responsibilities are divided between medical providers and patients under PIPEDA is that if patients do not know that their personal information has not been fully protected, then there is no obligation for medical providers to actually take actions if they are concerned that patient data might be stolen unless a complaint is filed. A medical provider might believe that some patient information was stolen, but might not be motivated to report the event if a patient has not discovered it. In other words, if it is believed that no harm was caused to a patient, then there may be no motivation on the part of a medical provider to make him or herself or the practice look bad and potentially face liabilities by reporting it.

The responsibilities placed on patients to essentially monitor whether parties, that have no need for the information, have obtained their personal information are worth noting given the

issue of digital privacy. At a time when electronic medical records have become the norm for most practices and hospitals, as well as most third parties such as insurance companies and pharmacies, the burden placed on patients is great. It is certainly true that medical providers and third parties face the burden of implementing measures to protect patient data. However, patients cannot assume that those entities are responsible for making it known if some type of data breach has occurred. Instead, that responsibility falls to them.

Even more, within a digital framework, the responsibilities and issues of protecting patient data under PIPEDA are unchanged. What is meant by this is that regardless of whether patient data are maintained on paper records or electronic records, the responsibility of medical providers and third parties is to limit access to those electronic records to only those individuals that need access. In addition, medical providers and third parties must ensure that the data is protected, so that the data is not intercepted over a wireless network like Bluetooth, Wi-Fi, NFC, cellular and RFID (Hung, Andrade, Chen, Huang, Martin & Zheng, 2007).

Overall, the information that has been examined about patient privacy has not been solely about the legal framework that exists in Canada with regards to privacy. PIPEDA was created not only for the medical industry, but also for all organizations conducting business within Canada. PHIA, unlike PIPEDA, requires that health organizations using personal health information for health purposes to report breaches of information. As has been noted, the concept of personally identifiable information is one that is worth understanding as not all information that patients might consider to be personal might be identifiable. If the information does not allow them to be identified by others, then it is not protected under PIPEDA or PHIA. The expectation of patients with regards to the information that should be protected might be incorrect given the legal framework that exists.

Furthermore, patients have responsibilities under PIPEDA that might also not be fully understood. Patients have the responsibility of initiating investigations regarding the misuse or theft of their personal information by filing complaints with the providers or entities that collected the information. The burden of constantly monitoring whether data have indeed been stolen, even if the theft was not known, is not within the realm of responsibilities of medical providers and third parties. In the era of EHR and digital data, this burden that has been placed on patients may make it difficult for them to ever know if their personal information has been stolen or misused. At the same time, this would seem to remove some of the burden for data protection from medical providers and third parties. If stolen or misused data never has an noticeable impact on patients, then there is no real motivation to announce that data were stolen or misused.

2.6 Summary

The purpose of this chapter has been to provide a review of literature related to the major themes and concepts that have been identified as important in the examination of the enhancement of digital privacy within an ubiquitous health care setting. The proliferation of electronic health care records is an important part of the health care setting in Canada. Medical providers, hospitals, and other companies have moved toward the use of EHR as a means of improving efficiency, reducing costs, and allowing for the easy sharing and access to patient information. The move toward EHR provide the benefit to patients of receiving a higher continuity of care as their records can be easily shared with all of their physicians and medical providers.

The use of EHR has also increased the use of cloud computing technologies by medical providers and other companies in the health care industry. Cloud computing allows medical

providers to utilize applications and databases from servers that are owned and operated by other companies as a means of reducing IT costs to their businesses. Cloud computing makes it possible for physicians and medical providers to access patient data from nearly any location with Internet access. The benefits include 1) patients being able to access health care services outside of traditional medical office, 2) the potential for greater collaboration on medical issues, 3) an increase in data collection, therefore the potential for better health care with real-time data collection and analysis is available and 4) faster response times, due to EHR shared amongst multiple offices.

Even within the medical office, the use of EHR combined with cloud computing is further enhanced with the use of tablets and other smart devices. Physicians no longer have to find a computer to review medical files. Instead, physicians can access patient data in front of the patient. Physician and medical professionals can also enter patient information in real time, which ensures that patient records are as up to date as possible. The use of tablets and smart devices for inputting and retrieving patient data also makes it possible to reduce medical errors that might otherwise occur if patient information were not entirely available at the time of providing care.

The expansion of digital technologies, however, does increase concerns about the privacy of patient information. The idea of patient privacy cannot be just about preventing hackers from gathering EHR over the Internet, but also about the policies and procedures of the many companies and providers that may access any single patient's records in the course of the full range of care that is given. Over the past decade, privacy regulations for medical providers and related third parties have been increased with the implementation of PIPEDA and more recent acts like Nova Scotia's PHIA. Companies and entities that collect personal information are

required to ensure that the information is protected and is only shared with others that need the information after receiving consent from the individual. While PIPEDA may seem to provide strong protections for patient data, the reality is that there are some concerns. First, PIPEDA requires that personally identifiable information be protected, which can raise issues about what patients and medical professionals consider to be personally identifiable information. Next, it is the responsibility of patients to initiate complaints that the personal health information has been breached, even though the business has the 'option' to open an investigation. This responsibility does not rest with the medical providers, unlike PHIA, which offers provisions forcing that breaches be reported.

In the end, it is these issues that provide a basis for studying how digital privacy of patients can be enhanced, not only in Canada but also in emerging countries. Even in a country like Canada, there is a need to consider how digital privacy can be enhanced. This is important as use of digital technologies in health care becomes as ubiquitous as health care itself.

Chapter 3 ANALYSIS OF CANADIAN AND BRAZILIAN PRIVACY LAW

3.1 Introduction

The purpose of this chapter is twofold: to examine the privacy landscape of Brazil and to compare the privacy landscape of Brazil with that of Canada. The analysis of the Brazilian privacy landscape, particularly as it relates to EHR and digital privacy for patients is vital in order to be able to provide recommendations for how digital privacy in a ubiquitous health care setting can be improved in an emerging nation such as Brazil. While Brazil is gaining a great deal of attention as an emerging nation in South America, there are still many issues that are problematic in that country's health care system (Paim, Travassos, Almeida, Bahia & Macinko, 2011). Brazil is a country in which the use of EHR and the development of privacy rules and regulations to enhance digital privacy are truly in their infancy (Webster, 2011). For a country that has gained great attention in recent years as a major emerging nation of the world, the privacy landscape of Brazil, particularly as it relates to personal patient data and EHR, is lagging.

There is a benefit in understanding Canadian and Brazilian privacy laws, as the challenges that Brazil is now facing with in regards to protecting personal information are similar to the challenges that Canada began to address over a decade ago. The analysis that follows will demonstrate that while Brazil's legislation trails behind Canadian privacy legislation development, the two countries share similar paths in implementing EHR and actualizing the rules and protections to protect personal health information.

I first provide a broad overview about the Brazilian privacy landscape, or perhaps more appropriately, the limited privacy landscape that exists at the present time. Then, the relationship of the broad privacy landscape of Brazil to the privacy of medical records will be examined. The focus of this part of the analysis will be to demonstrate how privacy laws and rules in Brazil

impact EHR, and to identify any gaps that exist in protecting digital privacy in the ubiquitous health care setting. Finally, the comparison of the Brazilian and Canadian privacy landscapes will be discussed in order to understand the similarities and differences. The comparison will demonstrate that current Brazilian legislation has similarities to Canadian privacy laws that were passed over a decade ago. Brazilian privacy legislation development appears to be following a similar path to that of Canada; this is important due to the fact that Brazil has a similar health care system to Canada. One exception would be that Brazil's health care system, SUS, is used to maintain all public hospitals, health centers and laboratories (Novais, 2012). Brazilians use a SUS card (health care coverage card), which allows access to citizen's health care records in both public and private hospitals; Brazil also has a private health care component. Therefore, understanding privacy and healthcare in both counties is critical when creating a supporting framework for enhancing digital privacy for emerging nations.

3.2 Brazilian Privacy Landscape

There are limited data protection laws in place at the present time in Brazil (ThomsonReuters, 2013). The personal data protection legislation is continues to be debated in congress, with only limited progress made in 2014 (Doneda, 2014). Since Brazil lacks a specific personal data protection act, robust protections that include the digital data stored in EHR are at risk as there is little recourse if there is a breach. Brazil's senate and congress have only recently passed the Marco Civil da Internet legislation to address digital information as something that is different, or of a different concern from that of personal information, in general.

Within the Brazilian Constitution, the right to privacy and of private life are guaranteed to all citizens (Financier Worldwide, 2012). The country's constitution states that the right to privacy and a private life cannot be violated, and that any such violations bring with it the right

to seek compensation (Costa, 2012). The right to privacy is treated culturally as something that is fundamental to Brazilian life and that allows people to live honourably (Costa, 2012).

One of the questions that must be asked is whether there are any specific guarantees within the Brazilian Constitution, related to privacy, such as information that is collected, used and disclosed by health care organizations and professionals. Within the Brazilian Constitution, there is a clause that states that privacy extends to correspondence, telephone communications, and telegraphic data (ThomsonReuters, 2013). The only exception to this rule is in the case of a court ordering that communications be made public for the purpose of a criminal investigation. Article 5 of the country's Constitution provides further protections for the information that is transmitted to other individuals or entities. For the citizens of Brazil, a guaranteed right exists that communication in nearly any form is meant to be private between the parties for whom the communication occurred. Within Canada, the constitution had an amendment in 1982 with the addition of the Charter of Rights and Freedoms. Under the charter, there is the right to privacy, but this only offers a reasonable expectation of privacy against unreasonable search and seizure of property (Government of Canada, 2013).

At this point, it must be noted that while the Brazilian Constitution states that people have a right to privacy and that personal information is protected, there is no specific legal definition of the term "personal information" included in the Constitution, nor does it provide an explanation of what constitutes personal information (ThomsonReuters, 2013). Due to the lack of definition of what constitutes personal information, any information that is shared with another person or entity, is considered to be of a personal nature and is protected by the Brazilian Constitution.

From a critical standpoint, the argument could be made that the perceived reliance on a broad interpretation of what is meant by the concept of "personal information" could result in confusion when attempting to enforce privacy protections for the citizens of Brazil. The lack of definition of personal information could pose problems, for example, when large amounts of information are collected, used or disclosed by an entity, such as a hospital. This can also be problematic given that the Civil Code of Brazil states that the private life of a person cannot be violated, and that any violation that is reported allows a judge to take any necessary steps to prevent a person's right to privacy from being violated. The Brazilian Civil Code also states that any violation of the right to privacy allows the person whose privacy has been violated to seek damages for that violation (ThomsonReuters, 2013).

Further to the privacy landscape that is present in Brazil, based on the country's Constitution and its Civil Code, there are also privacy protections included in the country's Consumer Protection Code (ThomsonReuters, 2013). The importance of these privacy protections, in relation to health records in general, is that they require certain actions of companies that collect personal information from the public. First, the Consumer Protection Code states that consumers must have free access to their personal data regardless of whether it exists in files, on index cards, or in databases (ThomsonReuters, 2013). Companies that collect personal data from consumers must provide consumers with that data if they request access without any cost. An interesting aspect of the first section of Brazil's Consumer Protection Code, as it relates to privacy, is that personal information stored in databases is included in the law (ThomsonReuters, 2013). Thus far, there has been no specific indication about consumer privacy related to anything electronic in the country's Constitution or Civil Code. However, the country's Consumer Protection Code does make mention of databases as a source of storage of

personal information and a location from which consumers must be provided the information that is stored about them, if they so desire.

The Consumer Protection Code states that information maintained by companies must be objective in nature. The collected information cannot contain negative subjective comments for a period longer than 5 years. At the same time, the information must be clear and accurate. If information is created or updated about an individual, then that person needs to be contacted in writing (Presidency of the Republic, 2007). While some of these rules might not directly apply to hospitals and other medical facilities, they do strengthen the idea that information about individuals in a medical setting must be clear and completely objective.

A draft bill was introduced to Brazil's congress in 2011 and passed in 2014 and is called the Marco Civil da Internet (Marco Civil). It established Brazil's first set of Internet regulations. The Marco Civil proposed some of the same protection concepts that exist within privacy laws in Canada (Hunton & Williams, 2013). Marco Civil is composed of rules and regulations regarding the transfer of data, especially the transfer of personal data to entities outside of the country. The law would prohibit any transfers of personal data to others outside of Brazil without proper security measures. The importance of this bill was that it outlined net neutrality, personal data protections and the creation of a data protection authority. The personal data protection section of Marco Civil states that when information is stored about Brazilian citizens, it must comply with Brazilian law, secrecy and privacy rights no matter the location of the stored data. The Marco Civil was held up in congress, until the U.S. National Security Agency's PRISM was accused of allegations of unauthorized data collection. Canada also played a role in this event, with the NSA leak identifying that Canada was spying on Brazil's mines and energy sector (Globalresearch, 2013). Within months congress placed a new priority on the Marco Civil, by

expediting the passing and amending the bill, so it more closely matched EU Data Protection Directive 95/46/EC. After congress and the senate approved the bill's powers, Brazil's president Dilma Rousseff then enacted the Marco Civil on April 23, 2014. More recent drafts of the bill also provide provisions for security that adds standards to data protection when data leaves the country (Infojustice, 2014).

Privacy standards are established in Brazil from multiple sources, including the country's Constitution, Civil Code, Consumer Protection Act, the data protection authority and the Marco Civil. Interestingly all of the acts, bills and codes introduced before the Marco Civil, did not provide provisions that enable freedom of speech for Internet providers and users, the use of open technology and standards, protection of personal data, intermediary liability, data retention and accessibility, as Marco Civil does. Marco Civil bill also has regulations for data retention that force Internet Service Providers to keep metadata for 6 to 12 months (Infojustice, 2014). Furthermore, Marco Civil offers protection for Internet users in the form of disclosure of information, as consent is now required before information can be shared. The Brazilian government is now working towards a second bill, a personal data protection bill, which will provide more robust laws to govern digital data collection, use, and storage.

3.3 Brazilian Privacy of EHR

It may seem unnecessary to spend time specifically dealing with the privacy landscape of Brazil regarding EHR, given that there are limited personal privacy laws protecting Brazilians that are specifically related to digital data. However, it is worth briefly examining why the privacy landscape of Brazil may not include specific rules and regulations for digital data, especially the digital data contained within EHR. The health care system in Brazil is still developing; over the past 40 years, reforms have been made to make health care unified and

universal across the country. While major improvements in the health care infrastructure have occurred over the past four decades, the system is still highly fractured between the urban centers that have many hospitals and physicians and the rural areas that have limited medical facilities (Paim, Travassos, Almeida, Bahia & Macinko, 2011).

In a similar manner over the past few years, efforts have been made within the health care system in Brazil to implement EHR as a means of providing better care to patients (World Health Organization, 2006). One of the major initiatives to implement EHR uses open-source software as the basis of the records system in Brazil. The open-source EHR system, the SIGMA Saúde Health Information System, is being used by a large health information company in Sao Paulo that serves 14 million patients, and has data on a total of 20 million patients (Webster, 2011). This represents approximately 10% of the country's entire population, from across 702 health care facilities in the country (Webster, 2011).

At the present time, however, there are truly no concrete rules and guidelines for how medical companies are supposed to protect the privacy of the medical records of their patients stored in EHR (Financier World, 2012). Instead, EHR are largely an uncharted area in Brazil even as major attempts are occurring to implement EHR on a large scale across the country. Patients in Brazil are accustomed to the idea that paper medical records are giving way to electronic medical record (Financier World, 2012). At the same time, hospitals, physicians, and other companies in the medical industry are navigating EHR in a country in which there are limited digital privacy laws, and in which the privacy laws that apply to all companies and industries are fairly broad.

Perhaps not surprisingly, some of the efforts to implement digital privacy rules that would apply to EHR have caused controversy from companies in the health care industry, as well

as other industries. Some companies are concerned that digital privacy rules will create major costs for them related to the protection of the digital privacy of patients, and really consumers in all industries (Hunton & Williams, 2013). In this way, the landscape of digital privacy in Brazil is not merely related to a lack of understanding or use of digital technologies. Instead, the digital privacy landscape in Brazil is based on rapid changes in the use of technology, as well as concerns from companies about the costs to comply with new regulations.

Finally, some progress is being made regarding digital privacy rights and responsibilities for companies and for citizens in Brazil in the form on the Marco Civil. As has been noted, the Marco Civil has been passed, but the personal data protection bill has not, therefore elements to protect the collection, storage and retention for EHR are limited or non-existent at the current time (Hunton & Williams, 2013).

It also seems appropriate to note that with the current Marco Civil there is a specific data protection authority, the Brazilian Department of Consumer Protections and Defence (DPDC). The newly anointed powers for DPDC, in the terms of fining offenders of the new bill, took root with a 1.52 million euro fine that was issued because Oi, Brazil's largest telecom, was recoding and selling its subscriber browser data (Privacy Laws & Business, 2014). The Marco Civil, as enforced by DPDC, can offer either a warning or levy up to a 10% of the economic revenue in Brazil, temporary suspension of activities, or prohibition of activities. The new Marco Civil framework was built to be complimentary for the personal data protection act that is currently in debate with congress. However, with the limited digital privacy laws in Brazil to date, there are now some provisions to handle data breaches, but nothing specifically targeting how EHR might be handled, even if patients were aware that their personal data had been compromised in some way.

3.4 Comparison of Privacy landscape between Brazil and Canada

Similarities. With the examination and discussion of the privacy landscape in Brazil, and how that privacy landscape impacts digital privacy related to EHR, it is useful to compare and contrast some of the major issues in the privacy landscapes of Brazil and Canada. On the surface, it might seem that Brazil and Canada have little in common in terms of privacy landscape. The reality, however, is that there are some important similarities in the privacy landscapes between of the two countries.

Brazil is in the infancy of implementing digital privacy laws and regulations. However, about 15 years ago, Canada was on a similar path. PIPEDA was implemented in Canada not with a focus on digital privacy, but with a focus on limiting the collection of personal information by government organizations (Samsuri, Ahmad & Ismail, 2011). A Decree was implemented in Brazil in May 2012 with a very similar goal: to regulate access to personal information on the part of the government's executive branch (Financier Worldwide, 2012). Therefore, Canada's path for implementing digital privacy protections was mirrored by Brazil, who is presently attempting to achieve the same types of protections.

Furthermore, another similarity in the privacy landscapes of the two countries is that both countries moved somewhat slowly to implement digital privacy protections. In Canada, the full implementation of PIPEDA to encompass digital privacy in all industries required about five years (Levin & Nicholson, 2005). This period of time did not include the time that was spent drafting and debating PIPEDA before it was implemented. In a similar manner, Brazil is in about the third year of true debate and negotiation related to proposals designed to provide protections related to digital privacy (Hunton & Williams, 2012). The country's government agencies, and the industries that will be impacted by new digital privacy regulations, are debating

how to implement digital privacy protections in a way that will benefit citizens without causing major harm to companies.

Personally identifiable information, under PIPEDA, is defined as information that can be used to help identify a person, but there can be disagreement about the type of information that can actually be used for identification (Adams, 2006). A person's name is certainly a means of identifying an individual. However, arguments could be made that a person's height or blood type are not useful in actually identifying a specific person, which would mean that those data are not protected under PIPEDA. While the inclusion of a definition of the type of personal information that is protected is a major difference between privacy laws in Canada as compared to Brazil, the actual data that are considered to be private can be debated. In Brazil, nearly every piece of personal information is considered private, but this is not explicitly indicated in the country's privacy laws (ThomsonReuters, 2012). In Canada, a definition of the type of data that are protected under PIPEDA is provided, but what can be considered personally identifiable information is still debated (Adams, 2006).

One other comparison to be made, between privacy laws in Canada and Brazil, involves the reporting of the theft or misuse of personal data on the part of a company and the responsibilities of consumers. In both Canada and Brazil, it is the responsibility of consumers and patients to report that their personal data has been stolen, or that their privacy as been violated (Bailey & Caidi, 2005; ThomsonReuters, 2012). If the information is classified as health information that is used for health purposes, provinces within Canada have additional acts like PHIA to shift the responsibility of the organization to report data theft. The privacy laws that are in place in both countries actually place a great deal of responsibility on the public to report when they feel their privacy rights have been violated.

In fact, companies and medical providers in Canada and Brazil have no burden to report that a breach of personal data has occurred under their respective federal acts (Bailey & Caidi, 2005; ThomsonReuters, 2012). This means that if companies experience a breach of personal data and no consumer recognizes a personal harm because of the breach, the companies involved in the data breach may never face any type of penalty. In order for any investigation to occur, within Canada, it is normally the consumer or OPC that opens a complaint. Brazil has a similar process in that the consumer or data authority will normally start an investigation.

Differences. One area of the privacy landscape in which differences exist between Canada and Brazil is the requirement for companies and particularly medical providers to protect patient data. In Brazil, companies and industries are required to protect consumer data when transferring data outside of Brazil, but no specific requirements are included in the privacy laws about how to actually protect that data (ThomsonReuters, 2012). Instead, companies have a great deal of freedom to implement protections and decide how to protect consumer data even with the passing of the Marco Civil.

In contrast, PIPEDA sets out a number of rules about how data, particularly electronic data are to be treated, exchanged with other companies, and secured to prevent data breaches (Kerr & Caulfield, 2008; Peyton, Hu, Doshi & Seguin, 2007). Companies in Canada are required to not only know their own data protection methods, but to also know the data protection methods of third party data providers, that they hire. As discussed, PHIA and PIPEDA are governing privacy laws for Canadian health care providers. PHIA, which is legislation for privacy and health care in Nova Scotia, will be the governing privacy law, once the Nova Scotia government completes an application for the federal government to remove the protections of PIPEDA. At such time, when the application is successful, health care providers

operating in Nova Scotia will need to comply with PHIA alone (APNS, 2013). A physician who shares information concerning an individual, either living or deceased, must be cautious that the information cannot be used to identify that person. There are a few exceptions, under PHIA, in which using information that could identify an individual would be acceptable. These instances include if the information was used to process a payment, to help plan a health management system (such as an EHR), or planning a program or service (APNS, 2013).

The differences in rules and guidelines about how companies and providers have to protect data in Canada and Brazil demonstrates that Canada has had more time to develop rules related to privacy and data protection. Another way of thinking about the difference in specific rules about data protection between Canada and Brazil is that Canadian politicians and officials have taken the approach to privacy that companies need specific rules and guidelines to follow to protect consumer and patient data. In contrast, the Brazilian government has taken the approach to privacy that companies can monitor their own actions and determine how to protect consumer data with limited privacy rules on data transfer. However, this does seem likely to change in Brazil if any of the proposals that are now being debated in congress and the senate to address personal data protection pass into law. The most significant change in Brazilian law, covered in the Marco Civil, include specific rules about the actions that companies would have to take to protect digital data, such as Subsection III that would require that providers maintain logs regarding the individuals and entities that access data records (Doneda, 2014). As discussed, there are a number of specific penalties that can be enforced, if there is information shared without proper securities outside of Brazil.

3.5 Conclusion

There are a number of similarities and differences between privacy landscapes of Canada and Brazil. Table 1 shows the similarities and differences between the two nations. While the two countries are more than a decade apart in terms of the actual level of digital privacy laws that exist, the paths that they have taken to establish digital privacy laws are similar. In addition, ambiguity exists in the privacy laws of both countries about the specific personal data that are protected. While Canadian privacy laws include a specific definition of the type of data that are protected, they do not provide specific examples of what is meant by the personal data that are protected.

	Brazil	**Canada**
Similarities	• Slow implementation • Regulate access to personal information • Federal privacy legislation that does not force providers to report breach	• Slow implementation • Regulate access to personal information • Federal privacy legislation that does not force providers to report breach
Differences	• Lack of concrete definition of personal information • Marco Civil which covers data transferred out of country and some privacy legislation • DPDC has specific powers under the Marco Civil to fine and punish offenders	• Personal information is any recorded information about an identifiable individual • PIPEDA legislation covers the collection, use and disclosure of personal information in commercial activity • PHIA govern the collection, use, disclosure, storage and destruction of personal health information collected by health providers; also has provisions for fining • Privacy Commissioner's powers include investigation, audit, pursue court action, public reporting, public research and promote awareness

Table 1: Summary of Canadian and Brazilian Privacy Law

Businesses in both Canada and Brazil are not required to report data breaches, unless it is covered it under provincial acts like PHIA in Nova Scotia. The privacy commissioner of Canada is working to expand the protections for Canadians and does have a proposal to add breach notification as a stronger measure under PIPEDA (Office of the Privacy Commissioner, 2013). Instead, the responsibility of reporting privacy breaches lies with the consumers and patients who are impacted. Companies have no responsibilities to report data breaches, so it is possible that data breaches could go unreported if consumers and patients are not directly impacted by the breaches or are not aware that they have occurred.

The major difference in the privacy landscapes of the two countries involves the laws imposed upon companies about how to protect consumer data that is interpreted by Brazil's DPDC or Canada's Privacy Commissioner. In Canada, a list of rules and guidelines are provided about how companies are to protect consumer data under the Privacy Act, PIPEDA, and provincial acts like PHIA. In Brazil, the Marco Civil provides powers to the DPDC to levy warnings, fines or even halt operations of a corporation (Almedia Advogados, 2014).

The purpose of this chapter has been to conduct an analysis of the privacy landscapes of Canada and Brazil. The information examined in this chapter has demonstrated that Brazil has taken some necessary steps to protect privacy, but until the data protection act is passed, the Marco Civil provides limited privacy protections.

However, it is the comparison of the privacy landscapes in Canada and Brazil that allows us to understand the closing gap between privacy laws in both countries. Both countries have privacy laws that allow for a great deal of interpretation about what is specifically considered to be personal information. The information that is to be protected in both countries can be debated because of the broad terminology used in the privacy laws in Canada and Brazil. Furthermore,

both countries have recognized bodies with powers to help govern the growing body of privacy laws to help protect information. This understanding is important because it can help develop a supporting framework to augment privacy for organizations in both countries.

Chapter 4 CASE STUDY

4.1 Introduction

The purpose of this chapter is to present an analysis of the Brazilian hospital through an on-site workshop I participated in and two published research papers that were written by collaborating researchers. A case study will be fashioned, as a result of the analysis, to aid in the creation of a supporting privacy framework. The Brazilian Visual Analytics (BRAVA) initiative was an international collaboration between Canada and Brazil, sponsored by Boeing. The initiative drew dozens of researchers with a primary focus on visual analytics, in Brazil, and Canada. This provided an opportunity to build a flagship project that sponsored research between Dalhousie University, University of British Columbia, OCAD University and UFSCar's Advanced Interaction Laboratory that were focused on visual analytics in a mobile health care context. Previous research had been completed at the Brazilian hospital, before I joined the team. The data previously collected consisted of photos, videos, prototypes and notes that provided an insight into the hospital's operations. There were weekly meetings with the international research team, all of which provided an opportunity to review all collected data from both a Canadian and Brazilian privacy lens. I had a strong interest in Canadian privacy law that was cultivated by my participation in privacy law courses, completed during my degree at Dalhousie University, and further developed as an operations leader within a telecommunications company.

The workshop that was conducted at the Brazilian hospital provided a rare opportunity to collect primary research that could be augmented with secondary research that was previously collected. The secondary research was in the form of raw data from published research studies at the same Brazilian hospital. The workshop, held in August of 2013, and before the NSA's leak

of Canada's supposed role in corporate espionage, was completed onsite at C.A.I.S. Clemente Ferreira Hospital in Sao Paulo, Brazil. The workshop required a translator to relay information between the researchers and staff in the Brazilian hospital due to the Portuguese-English language barrier. Post workshop, I was fortunate that there were two researchers on exchange from Brazil at Dalhousie University, which provided an opportunity to review recordings of the workshop to verify the accuracy of information that was translated.

The information that has been examined thus far has provided an understanding of the laws and regulations related to digital privacy for patients in both Canada and Brazil, as well as the technical issues related to digital privacy. The Marco Civil, in Brazil, offers limited protection in the form of privacy of information, until such time that the personal data protection act is passed. However, hospitals in Brazil are adopting digital technology as a means of interacting with patients and collecting information about their care. The insufficient digital privacy protections in Brazil, combined with the emerging use of digital technologies, provided an interesting opportunity to examine this development in actual practice. The Brazilian hospital primarily relies on paper-based information procedures, therefore has not updated their institutional policies to address the emerging use of digital systems.

The participation in the workshop and the raw data from two published research papers, on the same Brazilian hospital, do allow use to draw broad conclusions about all hospitals in Brazil with regards to the use of digital technology and the protection of digital patient records. Instead, the goal of the analysis was to create a case study by reviewing previously collected data with a privacy lens in order to gain insights and understanding for the use of digital technologies and how digital privacy is used within the hospital. The limitations in conducting the workshop meant that 20 staff had been observed in a single unit of the hospital (i.e. the residents of

children's ward). The information gathered from the observations and interactions with the personnel in one single unit of a single hospital in Brazil provided a means by which to relate the theoretical and legal issues about digital privacy to actual practices of the medical facility. Furthermore, the information and analysis provided from the workshop and research papers will be used to discuss a supporting privacy framework that could work for organizations in Canada and emerging countries, like Brazil.

4.2 Research Paper Publications

The hospital began operations in 1955, providing treatment to people suffering from tuberculosis. The hospital's location (i.e. surrounded by woods and open areas) made it a perfect place for the treatment of tuberculosis at that time. In 1978, the hospital transitioned to providing psychiatric services to patients in the aftermath of suffering from tuberculosis. A further change was made in 1983, where the hospital transitioned to a true mental health facility. In 2000, the mental health facilities were expanded with a neurological unit for the treatment of children and adolescents with mental health issues. The nurse is responsible for interacting with the patients, and providing information to the therapist and team director; the nurse also manages patient medications and files. A second tier of nursing, the auxiliary nurse, handles the bathing of patients, administering medications, and assisting the nurse with other duties. Another important role within the facility is the professional therapist, who is responsible for providing various therapies to the patients, as well as meeting with the nurse and team director. The team director, for the facility has the role of coordinating the activities of the entire team and helping to solve problems involving treatments as they arise. (Anacleto & Fels, 2013)

The first publication, *Adoption and Appropriation: A Design Process from HCI Research at a Brazilian Neurological Hospital* (Anacleto & Fels, 2013) was focused on obtaining

information about the types of technology used by a single team at C.A.I.S. Clemente Ferreira Hospital and how technology was appropriated. To help the researchers avoid bias on how technology is used the study's methodology was a blend of using Participatory Design (PD) and Task Centered Design (TCD). PD is effective because it allows stakeholders to input information into the final design and when blended with TCD, there is also focus on the user and the tasks they need to perform. Anacleto & Fels research study was not directly focused on patient privacy, but there were a number of observations that will provide insights and understanding to digital privacy within the Brazilian hospital. The focus of their research was to provide a lens on how health professionals appropriate technology.

Appropriation occurs when something is created for one purpose and is repurposed for a different task. For instance, there was an example of a hospital worker using their personal cell phone to take pictures of a patient due to limited camera equipment. With a privacy lens, on issues such as this, questions need to be asked about the capture, use, storage, retrieval and disposal of personal information.

Anacleto & Fels captured the data in the hospital to assist in the documentation and treatment of the patient. My research, using a privacy lens and viewing the same raw data that was collected by Anacleto & Fels, takes into consideration the collection, use and disclosure of personal health information. A technology that was introduced during Anacleto & Fels research was the computers controlling public displays in common workrooms. This would allow the director of the hospital to announce emergency meeting on the large screen displays, which would save time compared to the current practice of individually calling employees to organize staff meetings. When visiting the site, and considering privacy, it was noted that the displays were installed in common areas where staff and residents were able to view the information;

therefore any agenda was not private.

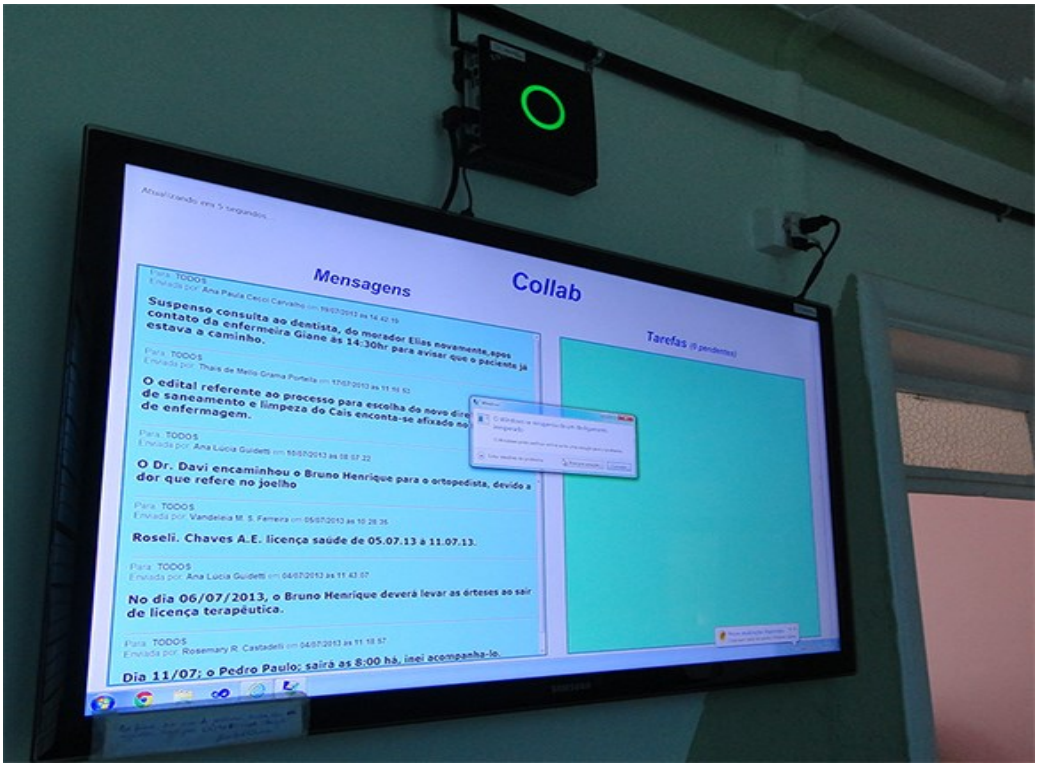

Figure 1: Public Displays in Hospital

The second publication, *Understanding NUI-supported Nomadic Social Places in a Brazilian Health Care Facility* (Anacleto & Fels, 2013) focused on natural socializing practices within a chronic care hospital and the environmental and informational practices that influence this social behavior. This was done in order to better understand how to design technologies in Brazil to support communities and sociability. The methodology was composed of an ethnographic study within the Brazilian hospital, by gathering data through shadowing 12 health care professionals over a period of one week. Four characteristics that were observed included 1) sociability 2) spontaneity 3) storytelling and 4) information. All of these characteristics helped researchers analyze the social network that promotes that sharing of information through

spontaneous meetings by storytelling, amongst the professional staff. The information shared by staff included workplace logbooks, patient files and new information technology systems. I am now going to present a number of key privacy concerns with these practices.

The risk of open information sharing within the hospital could potentially provide residents and staff members, for whom the information is not directed, access to data that should be out of scope. Access to medical information that is not required could leave data venerable that includes prescribed narcotics and patient well-being. While culture needs to be maintained, the government has made it clear through the Marco Civil and the proposed personal data protection act that is currently under senate and congress debate, that privacy has a strong place within Brazilian culture. As each country faces new challenges in the global marketplace, in some instances standards should to supersede cultural norms or that culture could be in jeopardy for failing to be competitive in the global economic marketplace. The open information sharing practices within the Brazilian hospital should to be considered, as the implementation of an Information and communications technology (ICT) system that mirrors today's practices could leave information accessible to a much wider audience than is necessary for patient care. In addition, open information practices need to adapt in order to protect personal information. Although there needs to be a balance between information sharing and privacy to be effective in the treatment of patients, adding an ICT system within the hospital would pose considerable privacy risks.

4.3 On-Site Workshop

The overarching research goal of working within the Brazilian hospital was to present prototypes for designing mobile support for long-term technological applications for institutional care providers. The research methods included user-centric participatory design, observation,

data capture through notes, video, voice recording and pictures, in addition to shadowing. As a researcher, my interest was privacy related, as I attempted to observe staff and residents in their natural institutional setting and probe how privacy and technology interconnect. The workshop was delivered over a three-day period by four researchers that were either delivering training, answering questions, providing technical support or shadowing a health care provider. A limitation of these sessions was the requirement of a translator, due to the English - Portuguese language barrier. To overcome this limitation there were two Brazilian students attending Dalhousie University that were able to verify the accuracy of the translations once they were recorded. The Brazilian students, completed the verification in Halifax, Nova Scotia by watching video of the workshop and creating a verification template for each video segment.

Hardware & Software	**Purpose**
Hardware: HP Slate 7 Tablet	Physical Tablet
Android version 4.2	Tablet's Operating System & Version
Voice Recorder	Used to record audio
Adobe Reader	Application used to read .PDF files
Evernote	Productivity Software was used to create both offline and online data to share information with members of your choice
Skitch	Used to Blur Photos
Camera Application	Capture Photo's on the tablets drive
Google Drive	Cloud Storage
Etch-a-sketch	Used to teach finger movements
Adduction!	Game to teach tablet use
aTilt 3D Labyrinth	Game used to teach tablet sensor functions

Table 2: Initial Tablet and Software Configuration

4.3.1 Day One

There were 20 tablets provided to 20 hospital staff participants with pre-loaded software and an electronic user guide that was translated into Portuguese. During training, hospital staff

was shown how to operate the tablet, while the researchers captured notes and assisted staff in using the tablets provided. The basics that were taught included 1) touch screen gestures to change screens and move applications, 2) how to record video and take pictures, 3) how to record audio, 4) how to add applications to the home screen and 5) how to retrieve files. The exercises were designed to engage the hospital staff by focusing on how to capture video, voice and file locations while taking privacy considerations taken into account. The first exercise was designed to have staff interview one another using audio and video and capture the data locally on the device. The second exercise included staff leaving the training room and entering the hospital to record something that was important to them, that would be later shared with the group. Day one also introduced a prototype that provided a feedback loop between the researchers and staff on a tool that could be used to help triage residents.

4.3.2 Day Two

Training sessions were provided for the use of Evernote, which is a productivity tool used for the capture, use and storage of information. Evernote is a good data capture application for typing short or long notes, storing pictures, and recording video and audio, all in an encrypted environment. We provided instructions on how to capture, link and complete minor editing for video and picture annotations when creating patient profiles during an exercise. During these exercises, instructions on how to create facial blurring were demonstrated within the application Skitch, to provide better privacy options when collecting patient information. Day two also had each of the tablets connected to an outside Internet connection, therefore Evernote could sync with a master account. Researchers could then review a master Evernote account at a later date to remotely review the usage of Evernote as a productivity tool within the hospital. At the end of day two, the hospital staff were asked to take the tablets home for use and become more familiar

with the basic functions before the final day of training.

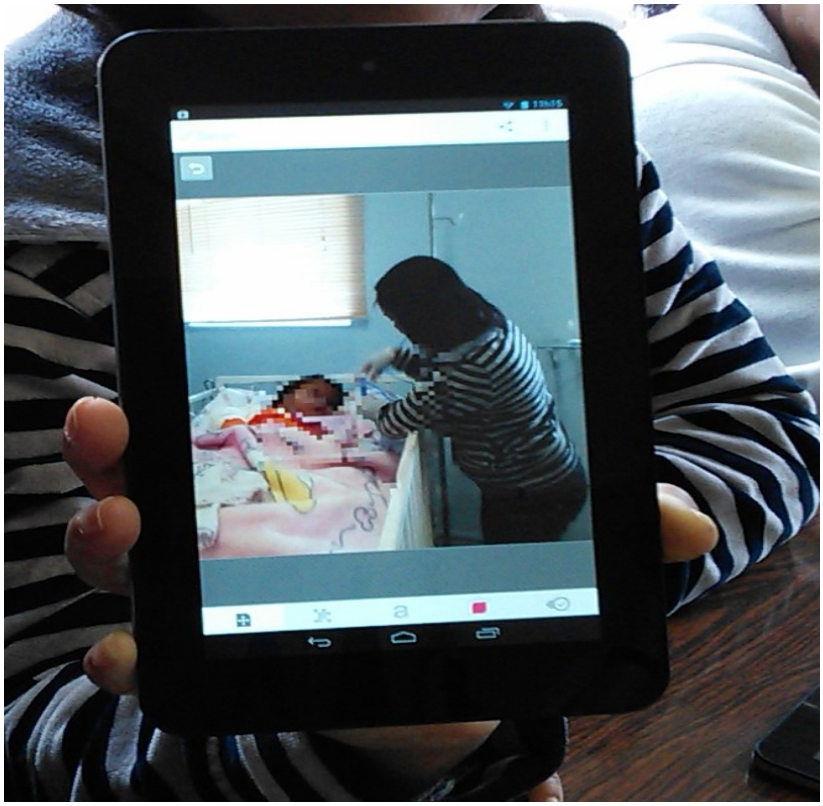

Figure 2: Facial Blurring Using Skitch

4.3.3 Day Three

Evernote's master account was checked, so researchers could review the information that was captured on day two and ensure it was synced and to review any new information that was uploaded. Day three included the introduction of two additional prototypes that were centered on iCare. ICare is a non-functional prototype to help provide insights on designing mobile support for long-term care facilities. These prototypes were mock-ups of applications for the Brazilian hospital and participants were able to provide feedback on their use and features they would like to see implemented. The workshop concluded with a plan to check on the use of the tablets to determine how the tablets were being used after the research team left the facility in

August of 2013.

Figure 3: Non-Functional Prototype Workshop Delivery

4.4 Challenges

The research team was faced with challenges during the workshop. The first challenge was the lack of availability of Internet connectivity, as the Internet connection was only available in the administrative office and not throughout the hospital. This presented difficulties during the workshop and on the second and third day, the staff had to move to the director's office to upload files from Evernote, browse, check email, or perform any other type of activity that required an Internet connection. The second issue was the wireless speed of the connection; it was slow and only provided connectivity of 1 MBps. This presented challenges for staff when they attempted to synch to Evernote, email and other on-line applications. Considering that a

small video would be 20-30 megabytes it size, uploading the video would take 10 minutes to complete. Another challenge, of the workshop was that many of the staff had never experienced touch technology before. The English Portuguese barrier also presented difficulties, when training or demonstrating technology, as there was a heavy reliance on the translator.

The workshop had three interactive components where the research team was able to observe the use of the tablets within the hospital environment. These activities included staff members 1) collecting information about a resident, 2) collecting information about what was most important to them and 3) providing information to the patients.

4.5 Case Study

The case study is a convergence of the two previously discussed published papers, including raw data from the publications and the workshop. The workshop and research practices will lay the groundwork to discuss findings and the integration into one case study. As a result, a supporting framework will emerge that consists of standards for enhancing privacy for Canadian and Brazilian organizations.

Appropriation can lead to serious privacy risks if devices are used to close gaps in current work processes, when attempting to improve processes. This can lead organizations vulnerable to privacy fines, the banning of their products and services or having large public reports publicized on how privacy was breached in countries where privacy breaches are enforced. Creating applications to mirror work practices can also create large breaches within an organization, when work practices may seem safe in small workgroups, but the same practices would open the potential for large data breaches on the Internet.

Within the Brazilian hospital there are small groups of people that socialize frequently, presenting information that was health related to one another. In addition, large volumes of

information are left unattended that contains resident prescriptions, dental, paediatric and neurological data, due to the hospital's pen and paper practices.

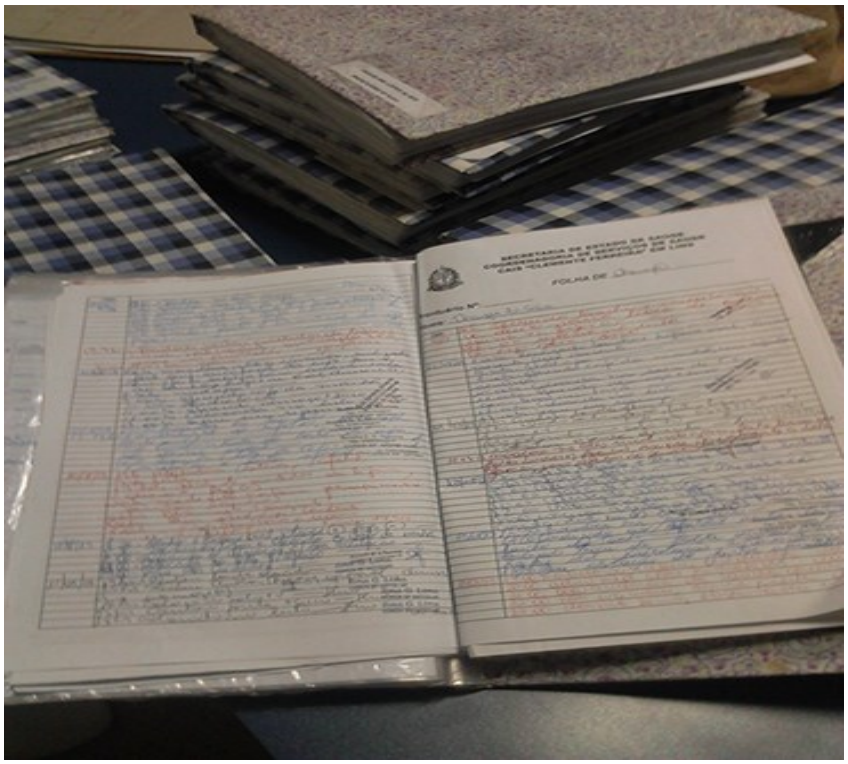

Figure 4: Volumes of Information at Hospital

Education is an effective form for creating best practices within the work environment as was demonstrated in the workshop. Presenting how to perform functions like blurring photos, keeping devices in secure locations and not bringing them home is a good first step for teaching privacy. This should lead to people thinking about privacy by adding screen lock passwords and as they become more comfortable with the technology, installing additional security applications. Privacy needs to be a set of conditions that compliment the environment, creating layers that make sense and promote good communication, professionalism and management skillsets.

4.6 Observations

A staff member was photographed taking a photo, during the course of their workday, of a patient in treatment at the Brazilian hospital. This can pose a privacy issue as the collection, use, disclosure and storage was not previously discussed with the patient. Therefore, the data had the potential to leave the hospital or, to be used, in a way not desired by the patient. Privacy breaches can also happen in another form, by simply using a device that was used for another official purpose or person. This was demonstrated within the research study of Anacleto & Fels, where the professional therapist used the tablets provided as a way to demonstrate information related to the conditions of the patients, as well as to allow for interactions between the patients and the therapist. The therapist used the tablets to show videos and illustrations to the patients as part of the therapy process. The nurses also used the same tablets when collecting information. The privacy risk associated with more than one staff member using a tablet, with no individual profile, leaves the potential for information breaches.

During the workshop, it was observed that more than one staff member was attempting to install a Facebook application during training. Post workshop, an analysis showed that the top three application categories that were installed on the tablets were games, entertainment and photo applications.

Within these categories popular image applications like Snapchat and Instagram were installed. Games included popular titles like Fruit Ninja, Angry Birds and Temple Run and entertainment had a number of Google and Kindle applications. When researching privacy application installs, only three security applications were loaded on the tablets. There were also a number of file browsers, note applications (e.g. Google Keep) and office applications. One of the applications was software designed to protect photos, another was for the purpose of locking

videos, and there was an application to lock the tablet, so that individuals would require a password to access the device.

Based on the observation and analysis that was completed, there appeared to be no special software or applications to secure patient information or files. However, it should be noted that most patient records were not in electronic format.

I also observed staff members during the workshop attempting to send email messages to each other with the tablets. In addition, the staff members were frequently observed visiting websites with the tablets during the workshop to test the browser functionality. However, within three months of the workshop, we checked the tablets remotely to see what applications had been installed (Table 3). The games category had grown to become the number one installed application type on the tablets, with 84 games installed across the 24 provided tablets to which 20 staff had access. The second largest growth area was entertainment, which experienced growth from the initial Etch-a-sketch install to include 60 new entertainment applications. This category is defined as applications that would provide personal or resident entertainment at the long-term care hospital children's ward where the initial research was completed.

This application installation analysis was completed, by checking a group Gmail account, that was initially setup to monitor application installations. Analysis installed applications also provided evidence that some of the tablets were taken out of the hospital, as there were pictures of building and events outside of the hospital setting.

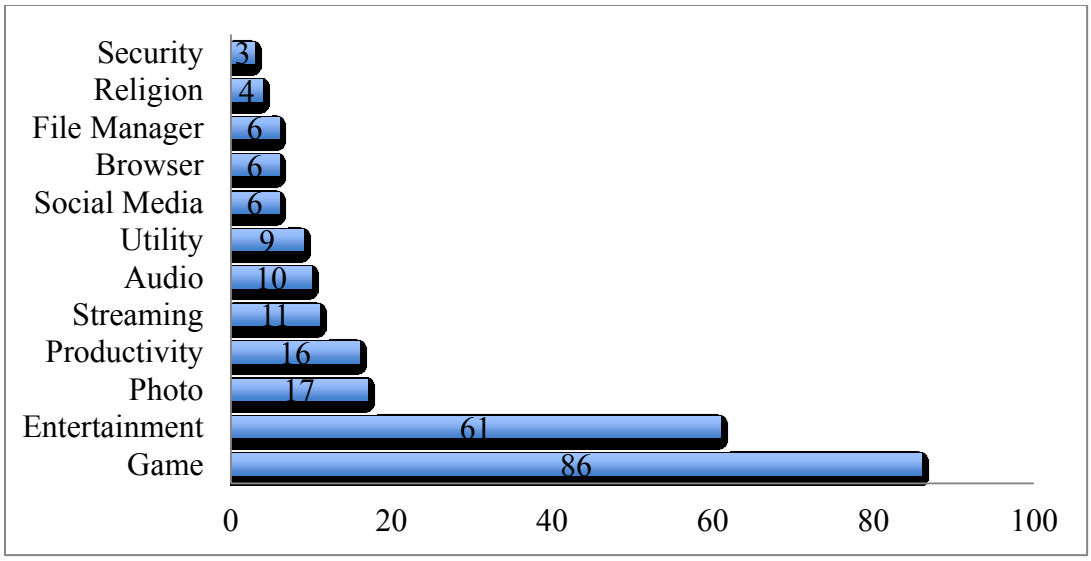

Table 3: Post-Workshop Application Installation

I observed a lack of security application installations and configuration on the tablets. On several occasions during the workshop, tablets were not secured by application, leaving the applications and information vulnerable. The tablets were occasionally left in unattended areas and this presents a physical security issue. It should be noted that tablets were generally only left in staff-only areas, therefore the tablets were kept away from patients, in most cases.

During the Anacleto & Fels research study, some patients were asked to watch videos on the tablets provided in their research study. The patients were sometimes left alone for brief periods of time to watch the videos without any staff member present. Patients who were observed using the tablets to watch videos or play games as part of their therapy appeared to enjoy the experience. The patients appeared to express happiness and interest in the information they gained from the videos, and interactions between the therapist and staff members seemed to be increased as a result of the use of the technology. The patients seemed to use the tablets for the purposes for which the staff members intended, which was to assist in the treatment process (Anacleto & Fels, 2013).

I observed that there was no specific procedure for securing the tablets provided during the workshop or, ensuring that they were charged and ready for future use. For example, the tablets were charged in one of the private workspaces located at a nurses' station, but no specific procedure seemed to exist about returning tablets to that specific spot when not in use. Instead, tablets were observed being freely handled to staff members, as they were needed. The only tracking process that I observed took place when a staff member did a physical count of the total number of tablets.

4.7 Analysis

Privacy applications were one of the least installed application types. A limitation of this analysis was that we could not review the tablets directly, as communications between the researchers and the hospital broke down in Fall 2013, after Canada was accused of spying on Brazil, a result of the NSA leak. The act of checking the group mailbox sent a security message to the hospital Gmail group account stating that the account had been accessed outside of their region, which caused additional friction between the researchers and the hospital staff. This practice was previously discussed and there were planned follow-up meetings with the hospital, but communications halted at this juncture. The security applications that were installed included "Video Locker" and "Hide Pictures – KeepSafe Vault". At some fundamental level, the hospital staff is interested in protecting the information on the tablets. The initial research team demonstrated to the hospital staff instructions on how to use the initial application suite, which included Skitch and how to blur facial features for privacy. Once the research team completed the workshop, staff members were responsible for attaching and uploading the photo, audio or video file within Evernote and deleting the original content from the tablet. Where the limited connectivity of one Mbps would make the task of uploading the large video files difficult,

employees have in a limited capacity, appropriated the use of the tablets to include local security. There were approximately eighty files contained on the Evernote account, that were a mix of videos and pictures uploaded at the time when the group Evernote account was analyzed. Due to the breakdown in hospital communications, there was no ability to check what was stored locally on the tablets.

The observations that were made at the C.A.I.S Clemente Ferreira Hospital cause some concerns and issues to be raised with regards to digital privacy. The primary issue of importance, based on the observations that were made within the hospital, was the lack of data privacy. The tablets were not protected physically or by secure application in a consistent manner to ensure that unauthorized individuals did not view sensitive, patient information. When providing the tablets, we did not provide a secure infrastructure nor, any rules of use to better protect the tablets, but we expected that continued communications with the hospital and researchers would continue; thus, these issues would have been addressed at a future date. As well, due to the previous pen and paper culture at the Brazilian hospital where patient records were easily accessible to staff, tablets were approached with the same level of security. Tablets had no local policy in place to protect the information that was stored.

The tablets did have sporadic application installs used to secure photos and videos, so there was some means by which to protect files. The issue of what is considered personal information and requires protection raises some of the issues that have been discussed in regards to patient privacy in both Brazil and Canada.

One of the issues that arose in the first research study and my observations was that the staff members of the hospital appeared to use the tablets without a great deal of concern as to whether files might be viewed by others. When the workshop was completed the Marco Civil

was not passed, but was under debate in conjunction with a personal data protection act. Since then, Canada was identified as committing espionage, based on the NSA leak.

Wi-Fi equipment was intentionally damaged at the Brazilian hospital, before the workshop and NSA leak, because there was suspicion that the equipment was being used to track staff. Due to the damage, future installs were placed high on the hospital walls to protect them from vandalism.

Figure 5: Wi-Fi Installed High in Hospital

With limited privacy regulations in Brazil, under the Marco Civil and the lack of a specific personal data protection act, the hospital and staff members were likely not violating any laws or rules in how they handled the tablets or the information on them. The argument could be made that some tablets had applications to protect the opening of videos and photos that used password authentication, thus demonstrated a requirement for data privacy. In this way, the

hospital and staff members had measures in place to ensure that others could not view the stored personal health information.

The tablets were provided to the hospital, during the workshop for productivity purposes, however personal information was found when analyzing the contents of the tablets; this presents an ethical issue regarding how professionals should handle personal health information, in general. Some tablets had a mix of personal and private information stored locally and on the group Gmail account, thus the hospital may be putting itself at risk with patient information being viewed by non-personnel. Storing the images and videos of patients on separate tablets would be a way to reduce the risk of patient information and data being viewed by others and creating a potential violation of patient privacy.

4.8 Conclusion

The information gained from the case study of a treatment unit at C.A.I.S. Clemente Ferreira Hospital demonstrated that while some efforts to protect patient information were in place, it is debatable whether those efforts offered adequate protection for personal health information. Staff members installed applications on the tablets that were used to protect images and videos of patients; this establishes that staff had some awareness of privacy issues. However, the tablets that contained patient information were also the same tablets that were removed from the hospital, by hospital staff. Furthermore, I observed that a specific protocol for physically storing the tablets did not appear to be in use by the staff members. The tablets were not used, at the time of this case study, to store full patient medical records, however, the information contained on them was medical and should be considered private in nature. In the end, this case study has raised important issues to consider when creating a supporting framework for digital privacy in Brazil.

Chapter 5 SUPPORTING PRIVACY FRAMEWORK

5.1 Introduction

The purpose of this chapter is to provide a supporting privacy framework for both Canada and Brazil that is based on the analysis of issues that have been identified through the literature review and discussed in the case study. A supporting privacy framework is appropriate, where privacy law frameworks in both Canada and Brazil have areas of focus that can be enhanced and offer value to organizations. Several specific areas of concern have been identified from the large amount of information that has been reviewed and examined thus far. The areas of concern can be broken down into 1) rules regarding the technology that are used in the ubiquitous health care setting; 2) the access to information and technology on the part of members of the health care organization; 3) the responsibility of providers regarding the protection of patient data, as well as responsibilities when a breach of patient data has occurred, and 4) the is personal data that needs to be protected. While it may seem somewhat simplistic to reduce all of the information and data that have been reviewed to four areas of interest, the reality is that these the four areas were continually identified. In this regard, the creation of a supporting privacy framework needs to be based on these four areas of concern.

In the discussion for a supporting privacy framework for Canada and Brazil, it must be understood that this supporting privacy framework is intended for organizations in both nations, even though their digital privacy protections are in different stages of development. Both countries have privacy law that can be enhanced by defining standards to ensure a reasonable baseline of digital privacy for patients in the ubiquitous health care setting. Canada's PIPEDA and PHIA offer federal and provincial protections in Nova Scotia, for instance, until PHIA is considered substantially similar to PIPEDA and Nova Scotia applies to remove PIPEDA for the

privacy of its health care records. The opportunity is to create a set of exact standards that require a yearly review, to set a balanced baseline for protecting health care records and enhance the already existing frameworks that are in place.

The discussion of the supporting digital privacy framework that is proposed is presented by discussing each of the four areas of concern that have been identified. Within each of the four areas, recommendations are made about how digital privacy can be enhanced to protect patient data. Recommendations are also made about specific rules or procedures that need to be mandated within each of the four areas of concern. It is important to recognize that while the analysis that has been conducted thus far has been based in research and investigation, the recommendations that are discussed in this chapter are intended to be realistic and for real-world implementation. The focus of this dissertation has moved from the theoretical, to the applied, in terms of recommendations though real-world laws, legal issues, and practices, that can be applied in actual practice for the medical communities in both Canada and Brazil.

5.2 Encryption Standards

The single most important issue involving the collection, use and disclosure of digital technologies of patient data may be protecting that data, to ensure that it is not intercepted or hacked (Fernandez-Aleman, Senor, Lozoya & Toval, 2013). Health care providers should be encouraged and even required to implement HER, and supporting digital technologies, to not only make it easier to collect and use patient data, but to also make it easier for patients to access their personal health information (Fernandez-Aleman, Senor, Lozoya & Toval, 2013). However, medical providers cannot simply trust a cloud computing company, or EHR provider, to provide adequate privacy when storing patient personal health information.

PIPEDA offers a guideline within section 4.7.3, under safeguard methods, that *suggests* encryption for records, but does not specifically offer a standard. Under PHIA, as discussed on novacotia.ca, "encryption and authentication minimizes the risk of access by unauthorized individuals" (Government Nova Scotia, 2013). An encryption standard, under both PIPEDA and PHIA has not been established for the minimum level of encryption that must be used to protect patient data. In addition, user access control has not been identified and is assumed; therefore a supporting could be implemented. The encryption should be specific to the collection, use, retrieval and storage of patient data over the Internet. The creation of a baseline requirement for how patient data could be encrypted locally and during transmission could be implemented to better protect personal health information. Thus, some assurances can be made by patients with the understanding that a standard of privacy is in place for data protection, regardless of whether the health care provider is a family physician or a hospital. The limitation for this recommendation is time sensitivity, where as Moore's law states that process speed or overall power doubles every two years, thus he ability to decrypt information increases, therefore the baseline supporting privacy recommendations need evaluation yearly (Encyclopaedia Britannica, 2013).

A privacy framework that addresses encryption and user access control could to be added to organizations that fall under PIPEDA and acts like Nova Scotia's PHIA, to help set standards for federal and provincial legislature. The supporting framework would set a standard and could be kept current by completing a yearly review.

Proposed supporting privacy framework. 1) The SHA-2, 256 bit standard ensures that information is not altered during transmit. Secure Hash Algorithm (SHA), SHA-2 in specific, is a set of cryptographic functions that were designed by the National Institute of Standards and

Technology and the National Security Agency to sign all digital certificates (Microsoft, 2014), 2) Advanced Encryption Standard (AES) creates a set of keys to make brute force close to impossible by altering the information in transit to zeros and ones. AES is a symmetric-key block cypher algorithm used to the same key is used for both encrypting and decrypting the data (McCaffery, 2003), 3) when the data is transmitted, Secure Socket Layer (SSL), provides a security standard for establishing an encrypted link between a server and a client. In addition, where SSL was the predecessor of TLS, both could be used interchangeably or in conjunction with one another, and 4) the use RBAC would provide user access control standards that can be implemented to limit access to information.

This supporting framework was chosen, based the research into security standards, the limited definitions that exist in Canada's PIPEDA and PHIA, Brazil's privacy legislation, published papers and workshop in a Brazilian health care facility. The workshop in Brazil, raw data from two published research papers and the research into privacy law in both countries provided significant evidence there is a need for a standard when an organization is attempting to protect the transmission and access to personal information. As discussed, Canada's PIPEDA and PHIA have specifically stated that personal information must be encrypted, as a requirement to protect personal information, but there are no exact measures that state what encryption standards should be implemented. It is reasonable that the law does not specifically set a baseline for encryption and user access control, whereby it would be expensive and time consuming to update the privacy legislation each time a new security protocol became a market standard; therefore the reasonable person test exists. By providing standards for today by implementing a supporting framework that is flexible, large or small organizations can ensure cloud-computing companies and EHR providers offer reasonable privacy standards. Additional

supporting evidence also suggests, from the workshop and published papers in Brazil that access controls need to be managed. Where the focus was on health care providers, role-based information access systems could provide sufficient controls for large EHR databases and small office environments. As health care organizations move data to the cloud for the collection, use and storage of information, balancing privacy becomes critical in accessing and protecting personal information. Although there are exceptions where PHIA, PIPEDA and the Marco Civil do not protect personal information, there is also a reliance on ethical standards that health care providers need to follow in order to protect personal health information.

There are a number of challenges for encryption that do not begin at the technology level, but exist the user level. The design of interfaces that are difficult to navigate can cause users to use alternate systems that are less secure to collect, use and disclose personal information. A usability evaluation, that was completed in 1999, stated that "user errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-non-existent" (Whitten, 1999). The creation of bug free code, so users don't experiences application freezing and crashes, helps the user experience. Limiting what users can alter, like security options for transfer or completing forms that are missing information will help ensure that the data is handled in a more secure and complete fashion (Whitten, 1999). Furthermore, the creation of a framework that includes standards for encryption and user access control, through good design, could make the adoption of a supporting privacy framework a easier transition by health care providers and the data providers they choose to use. The benefit of a supporting framework would be organizations would be offered a level of confidence knowing that patient data was protected at a reasonable level when utilizing services from a reputable cloud computing and EHR providers.

5.3 Information and Technology Access

An issue that was identified as being potentially problematic, during my observations within the health care facility in Brazil, was the lack of specific standards and practices for securing tablets physically and by software application. In Canada, privacy laws legislate the protection of patient data without addressing specifics about how electronic devices and computers are used to collect, use and disclose personal information. Medical providers may not recognize the risk of leaving a tablet or other electronic device unattended can therefore lead to theft or breach of personal health information. A nurse located in Toronto, in 2010, lost a memory stick containing 83,000 records of people who had flu shots (Cook, 2010). As previously discussed, there was another incident where 620,000 health records of Albertans were stolen. The issue of stolen or lost data is ubiquitous, as Home Depot reported it lost 56 million debit and credit card accounts in April of 2014 (Banjo, 2014).

The privacy framework for digital patient privacy in Canada and Brazil could include rules that require that tablets and other electronic devices used to collect and retrieve patient data be secured when not in use. This could be controlled through role-based access control (RBAC), which offers access based on the role(s) that authorized members require for accessing information (Deng & Zhou, 2012**).** RBAC would limit the access by ensuring that role based cannot be part of two groups in conflict. For instance prescribing and distributing pharmaceuticals would not be allowed, so a physician could have the role of diagnosis and prescribing a drug, but not the ability to distribute within an EHR. Physical security is also important, where members of medical provider organizations could be required to keep electronic devices they are using within their possession at all times and return them to a secured room or area when not in use. Rose based access and authentication would add a layer of

security for employees who leave electronic devices unattended or in a situation in which they could be stolen or misused by people who should not have access to patient data or EHR.

There are many different applications that can be used to lock an operating system, create a partition on a device and RBAC has role-based access that could support both options. Therefore, a device could have multiple purposes, i.e. gaming for patients and accessing health information, or be locked to one primary purpose. The medical professionals who were observed during the workshop, at the health care facility in Brazil, used the same tablets for multiple purposes, including collecting and storing information about patients and allowing other staff members to access the same device. In addition, post workshop, analysis of the devices that were provided during the workshop provided evidence that the devices had hundreds of applications installed and were taken to private residences to take photos and videos.

5.4 Provider Responsibilities

Medical providers in Canada are not required to report breaches of patient data under PIPEDA (Nisker, 2006). Instead, the onus of responsibility is with those individuals whose personal information was breached or the OPC can open an investigation if there are enough reports. More recent legislation, like Nova Scotia's PHIA, has legislation that limits the reporting of breaches to 'harmed or embarrassed'; patients may never be aware of the data loss if of these two situations have not occurred. Brazil also has similar limitations, within its privacy legislation, where information breaches do not have to be reported.

In both countries, the privacy laws related to patient data in the ubiquitous health care setting need to be more inclusive and require that medical providers report when they are aware of any information breach. To simplify the process for the collection, use and disclosure in information, all information collected from individuals should be classified as personal

information. Subjective viewpoints of individuals present too much variance for what would be classified as personal health information. Ethics is also an important factor, where a high ethical standard exists in most cases, there needs to be more communication to coach for what is acceptable for the collection, use and disclosure of information. Without ethics, issues like stocking, identity theft or snooping can happen, such as the case in Regina in 2012 (CBC, 2013). There were several health care workers who were caught snooping into co-workers confidential records. One of the workers, in the health care facility, stated that it is commonplace and appeared to be part of the culture. The issue was widespread, to the extent that the Saskatchewan privacy minister called it a chronic issue.

5.5 Personal Data

In Brazil, there is some question about what is classified as personal or identifiable information, and thus is protected under the existing privacy law. Canada has definitions for personal information, under PIPEDA and personal health information, as defined under PHIA. The issue that can be argued about whether something such as eye color or blood type is really personal data is the subjective nature of the individuals collecting, storing and disclosing information. By itself, information can appear to not create an identity, but with the development of new aggregate data applications, this is changing rapidly. Sites such as Facebook, Google Plus and any other site that creates a data profile by collecting, storing and disclosing information opens a new data point for that person, and therefore increases the risk of connecting other information that may harm or embarrass an individual.

As previously discussed, the use of RBAC for user access control in conjunction with the three-encryption methods (SHA-2, SSH, SSL/ TSL), could present a framework and establish a standard of protection for protecting personal health information. Technology, both wearable

and fixed sensors in health care facilities, can track heart rate, fitness, glucose levels, blood pressure and a host of other vital personal information, thus the data needs to be secure. The concept that digital information is secure and will remain private, like pen and paper records is not accurate, where the potential access remotely has increased significantly with cloud storage and local digital storage. In the move to EHR, patient data would be stored in server cluster; therefore that data can be shared and now has more potential for breach with an increase in access points. Currently, within Nova Scotia, PIPEDA and PHIA attempt to balance the sharing of personal health records and offer a layer of privacy for patient information in addition to a channel to request personal information. Through PHIA specifically, there is also an option to request a record of who has accessed personal health information.

5.6 Conclusion

Based on the information and data examined in this dissertation, a supporting digital privacy framework that includes encryption and access controls for Canada and Brazil have been discussed. There is a need to offer a framework that defines and standardizes the encryption and user access control during the collection, use and disclosure of personal health information.

	Canada	Brazil
Regional Privacy Law/Act	(Yes) PIPEDA and within Nova Scotia, PHIA	(Yes) Marco Civil Act
Encryption		
SHA-2, 256 bit	No	No
AES	No	No
SSL and/or TSL	No	No
User Access Control		
RBAC	No	No

Table 4: Encryption and User Access Control

The encryption framework should include 1) SHA-2, 256 bit, 2) Advanced Encryption Standard (AES), 3) SSL and/or TLS and 4) access control would be managed using RBAC. In addition, Brazilian medical providers would need to adopt provisions to report data breaches and a similar framework to PHIA, once the application has been completed by the Nova Scotia government and approved by the federal government of Canada. These security measures are specifically purposed to increase the protection and security of patient data, therefore increasing the responsibility of medical providers to protect patient data and report breaches of patient data, and provide specifics about what constitutes personal and identifiable patient data. Medical providers should be responsible for securing the tablets and other electronic devices on which patient data are recorded and retrieved. Medical providers should not use the same devices on which they record and retrieve patient data for other purposes. The devices on which patient data are recorded should be used solely for the purpose of recording and retrieving patient data. In addition, electronic devices should have to be secured so that other people are unable to use those devices to potentially gain access to confidential patient data.

Medical providers should also have the responsibility of reporting any breaches of patient data. At the present time, medical providers in Canada and Brazil do not have the burden of

reporting data breaches. Patients should not be responsible for reporting data breaches once they discover that their personal data has been stole and others have misused it. Finally, specific definitions of what constitutes personal data should be put into law, and that definition should be any piece of information or data collected by medical providers.

Chapter 6 CONCLUSION

The aim of this research was to propose recommendations to enhance digital privacy by introducing encryption and access controls that can be used within Canada's health care system that includes components that can be adapted to the health care systems of emerging nations. As part of the aim of this research, one of the underlying objectives was to understand the privacy issues and concerns that are currently part of the health care systems in Canada and Brazil with regards to digital records. Another objective of this research was to understand the ubiquitous technology that is part of the process of digitally capturing, storing, and sharing patient information.

The proliferation of electronic health care records is an important part of the health care setting in Canada. Medical providers, hospitals, and other companies have moved toward the use of EHR as a means of improving efficiency, reducing costs, and allowing for the easy sharing and access to patient information. The move toward EHR provides the benefit to patients for receiving a higher continuity of care as a large physician base and other medical providers can easily share personal health information. Due to the adoption of EHR in Canada, privacy regulations for medical providers and related third parties have been increased with the implementation of PIPEDA and more recent acts such as Nova Scotia's PHIA. Companies and entities that collect personal information collected are required to ensure that the information is protected and is only shared with others that need the information after receiving consent from the individual. While PIPEDA may seem to provide strong protections for patient data, the reality is that there are some problems. First, PIPEDA requires that personally identifiable information be protected. This can raise issues about what data patients and medical professionals consider being personally identifiable information. Next, there is no requirement

for organizations to report privacy breaches under PIPEDA. PIPEDA was designed to protect information during commercial transactions and set legislation in place for online transactions. PHIA differs in that it focuses on personal health information and places the responsibility on agents and custodians to report privacy breaches and has the ability to levy fines.

In Brazil, the move away from paper medical records and toward EHR has only just begun. Within the last year, the Marco Civil was passed that has created limited privacy protections, but the country still lacks a digital privacy protections act. Brazil is trending towards implementing concrete rules and regulations that truly provide for the protection of patient data. The proposals that have been discussed within the Brazilian Government are still being debated, but there is now some urgency as observed with the passing of the Marco Civil due to the NSA information leak.

While Canada and Brazil may seem to be many years apart in terms of digital privacy laws for the health care setting, the reality is that both countries share important similarities in terms of issues and concerns about digital privacy in the ubiquitous health care setting. Both countries have privacy laws that allow for a great deal of interpretation about what is specifically considered to be personal information. The information that is to be private information in both countries can be debated because of the broad terminology used in the privacy laws in Canada and Brazil. Furthermore, both countries place the burden of reporting privacy violations on consumers rather than on the companies that collect personal data, except in provinces where PHIA has recently been implemented.

Finally, the data we collected from the workshop at the C.A.I.S. Ferreira Hospital in Brazil and previous research completed by collaborating researchers at the hospital revealed emerging privacy concerns in Brazil. While some efforts were in place to protect patient data,

some of the ways in which digital technology were being used created risks for data breaches within the Brazilian hospital. For example, some staff members installed applications and passwords on the tablets to protect images and videos of patients. However, there were instances where the tablets that contained personal health information were taken out of the hospital and used for personal use. Furthermore, a specific protocol for storing the tablets did not appear to be in use by the staff members.

6.1 Supporting Privacy Framework

Based on the information and data examined in this dissertation, a supporting digital privacy framework was suggested for Canada and Brazil that has been designed to increase the protection and security of personal health information. This supporting framework would increase the responsibility of medical providers to protect patient data and work with newer acts, like PHIA, when reporting breaches of personal health information and provide specifics about what could constitute a baseline for data encryption. One aspect of a supporting digital privacy framework for Canada and Brazil should be a set of standards for the encryption of EHR. Rules need to be established for the minimum level of encryption that must be used to protect patient data and reviewed yearly to ensure the standard is adequate to balance usability of information with encryption. The encryption rules should be specific to both the storage and retrieval of personal health information, as well as the transmission of patient data over the Internet. The creation of a minimum requirement for how patient data should be encrypted would allow patients to know that there is at least a baseline for how their data is protected.

The privacy framework for digital patient privacy in Canada and Brazil should also include rules that require that tablets and other electronic devices used to collect and retrieve patient data be secured at all times. Members of medical provider organizations should be

required to keep electronic devices they are using within their possession at all times and return them to a secured room or area when not in use. Employees of medical providers should not be allowed to leave electronic devices unattended or in a situation in which they could be stolen or misused by people who should not have access to patient data or EHR. Furthermore, the electronic devices on which patient data are collected and retrieved should only be used for that purpose, or partitioned, and should be authentication protected.

In both countries, privacy laws related to personal health information in the ubiquitous health care setting should be written to require that medical providers report when breaches of patient data have occurred. Although PHIA has a requirement to report data breaches, there are limits. Medical providers should be required to report breaches of patient data as soon as they are discovered, not when a patient reports that his or her personal information has been breached. Medical providers should have to report breaches of patient data regardless of whether the breach may result in embarrassment or harm to a patient, such as a patient's personal information being used for the purpose of identity theft.

Finally, it is recommended that privacy laws in both countries should include specific standards for what is considered to be personal information with regards to patient information and data. The easiest way in which to define what is personal or identifiable information in relation to patient data might be that any information obtained from a patient's health record is personal and identifiable, which would mean that the loss or theft of any of that data would constitute a breach of personal health information. In the move to EHR, all patient data are supposed to be stored together so that the data can be shared and transferred easily and completely between providers. In this regard, if one piece of patient information is stolen or lost, it would seem likely that more of that patient's information would have been lost or stolen.

6.2 Generalizing the Framework to Other Emerging Nations

The strength of this digital privacy framework is that it is relevant regardless of the country or organization question. One of the aims of this thesis was to create a supporting digital privacy framework that could be used in emerging nations. While the case study that was part of this research was conducted in Brazil, the observations that were made and the conclusions that were drawn are likely representative and reliable across most emerging nations. The lack of strong privacy laws and a supporting framework for digital privacy in the ubiquitous health care setting means that issues of how to define personal data and the way in which EHR should be encrypted and protected must be addressed.

The recommendations provided for a supporting digital privacy framework, for enhancing patient privacy in the ubiquitous health care setting, could be used as a foundation for most organizations where specific protocols are not listed. The supporting privacy framework represents enhancements to much larger and developed privacy frameworks. The issues that have been explored and that have been included in the supporting framework are not unique to any particular country or organization. The issues included in the privacy framework are still of concern in Canada, a country in which EHR and laws to protect EHR have been in place for a decade.

The supporting digital privacy framework that has been outlined in this thesis is strengthened by the fact that it was based, at least in part, on the existing privacy laws regarding EHR and digital data in Canada and Brazil. The framework also strengthens the existing privacy rules, with provisions to set and not suggest, encryption and user access control minimum standards. Canadian federal government has spent over 10 years implementing and updating PIPEDA, which impacts the health care industry, and then has recently added provincial acts like

PHIA to specifically protect personal health information. For a country such a Brazil that is only beginning its journey to fully implementing EHR and using digital technologies to collect and use patient data, relying on information and insights gained from a country that implemented privacy laws 10 years ahead in the process can be beneficial. The advances that have occurred in protecting digital privacy in the ubiquitous health care setting in a country such as Canada can be applied to the digital protection framework in an emerging nation. At the same time, the downsides and mistakes that have occurred in a country such as Canada can also be used as issues that should be avoided or changed for the digital protection framework in an emerging country.

6.3 Future Research

Several recommendations can be provided for additional research to expand upon the work and insights of this thesis. One recommendation for future research is to investigate the process that emerging countries have encountered in implementing digital privacy laws and regulations related to EHR. The examination of the processes of implementing digital privacy protections in Canada and Brazil were informative in gaining an understanding of the issues and concerns that are present with privacy protections for patients in both countries. The comparison of the digital frameworks of both countries also allowed for an understanding that there were many similarities between the two countries with regards to digital privacy protections.

Another recommendation for future research is to compare the digital privacy frameworks regarding patient privacy and data protection across several developed nations. Comparing the digital privacy frameworks as they relate to the health care industries in Canada, the United States, the European Union (EU), and Japan, for example, would allow for greater insights into how these nations are similar and different in terms of the rules and regulations that

dictate how medical providers must handle and protect personal health information. The European Commission (EC) Directive on Data Protection applies to the processing of personal information. The directive imposes general rules as to the quality of data, the rights of data subjects, access to data, confidentiality and security in processing (European Commission, 2014). The Directive also states that is it not to share data with Countries that do not have adequate protection. The EU has also allowed trading information with Canada, due to the adequate data protection provisions in PIPEDA.

By comparing the digital privacy frameworks for the protection of personal health information across these developed nations, it might be possible to create a digital privacy framework for emerging nations that can capitalize on previous successes and failures. One other recommendation for future research is to investigate the issue of digital privacy within the ubiquitous health care setting from the standpoint of medical providers, particularly medical providers in emerging countries. Implementing strong protections regarding EHR may seem like a matter of simply creating standardized rules for how EHR should be collected, used, disclosed, stored and destroyed, but it is not. In reality, however, medical providers in emerging nations may not fully understand or appreciate the many issues and responsibilities that are associated with protecting personal health information in a digital environment. Another issue that needs to be considered is that the health care system does not have unlimited resources and cost of implementing privacy law is a significant factor. Gaining an understanding of how medical providers in emerging countries understand and perceive digital privacy issues would be beneficial in implementing programs to help improve digital privacy.

BIBLIOGRAPHY

Adams, C. (2006). A classification for privacy techniques. *University of Ottawa Law & Technology Journal*, *3*(1), 35-52.

Almeida Advogados. (2014). Data Protection in Brazil. The First Analysis of the Matter by The Consumer Protection Department. Retrieved from http://www.almeidalaw.com.br/download/A%20Definicao%20das%20Bases%20da%20Protecao%20de%20Dados%20no%20Brasil_ing.pdf

Anacleto, J., & Fels, S. (2013). Adoption and Appropiation: A Design Process from HCI Research at a Brazilian Neurological Hospital

Angst, C. M., & Agarwal, R. (2009). Adoption of EHR in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly*, *33*(2), 339-370.

Association of Psychologists of Nova Scotia (APNS). (2013). Personal Health Information Act Overview. Retrieved from http://www.apns.ca/documents/PHIAPresentationApril2013.pdf

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I. & Zaharia, M. (2009). Above the clouds: A Berkeley view of cloud computing. *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*, 1-28.

Arunachalan, B., Diamond, S., Chevalier, F., Szigeti, S., Stevens, A., Ghaderi, M., Talai, B. and Reilly, D. Designing Portable Solutions to Support Collaborative Workflow in Long-Term Care: a Five Point Strategy. In proceedings of CSCW-D 2014

Bailey, S. G., & Caidi, N. (2005). How much is too little? Privacy and smart cards in Hong Kong and Ontario. *Journal of information science*, *31*(5), 354-364.

Ball, M. J., Carla Smith, N. C. M. N., & Bakalar, R. S. (2007). Personal health records: empowering consumers. *Journal of Health care Information Management—Vol*, *21*(1), 76-86.

Banjo, S. (2014). Home Depot Hackers Exposed 53 Million Email Addresses. *The Wall Street Journal*. Retrieved from http://online.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282

Bolton, L. B., Gassert, C. A., & Cipriano, P. F. (2008). Smart technology, enduring solutions. *Journal of Health Information Management*, *22*(4), 24-30.

Boonstra, A., & Broekhuis, M. (2010). Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. *BMC health services research*, *10*(1), 231-248.

Bennet, Dean. (2014). Laptop stolen Alberta Health Information Stolen; 620,00 Records. Retrieved from http://www.huffingtonpost.ca/2014/01/22/alberta-health-information-laptop-stolen_n_4647386.html

Canadian Broadcasting Corporation (CBC). (2013). Report slams snooping by Regina health-care workers. Retrieved from http://www.cbc.ca/news/canada/saskatchewan/story/2013/02/12/sk-health-care-privacy-1302.html

Cook, M. (2010). Ontario healh privacy compromised by memory stick loss. Retrived from http://www.bioedge.org/index.php/bioethics/bioethics_article/ontario_health_privacy_compromised_by_memory_stick_loss

Costa, L. (2012). A Brief Analysis of Data Protection Law in Brazil. Retrieved from http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/Report%20(June%204th%202012)%20-%20A%20brief%20analysis%20of%20DP%20in%20Brazil%20(updated%20version).pdf.

Cucoranu, I. C., Parwani, A. V., West, A. J., Romero-Lauro, G., Nauman, K., Carter, A. B., ... & Pantanowitz, L. (2013). Privacy and security of patient data in the pathology laboratory. *Journal of pathology informatics*, *4*, 23-39.

Deng, W., Zhou, Z. (2012). A Flexible RBAC Model Based on Trust in Open System. Proceedings of the 2012 Thurd Global Congress on Intelligent Systems, 400-404. Retrieved from http://dl.acm.org/citation.cfm?id=2417935

DoctorsNS. (2014). Privacy Legislation. Retrieved from http://www.doctorsns.com/en/home/practiceresources/privacy-legislation/default.aspx

Doneda, D. (2014). Privacy and Data Protection in the Marco Civil da Internet (Brazilian Civil Rights Framework for the Internet Bill). Retrieved from http://www.privacylatam.com/?p=239.

Doukas, C., Pliakas, T., & Maglogiannis, I. (2010, August). Mobile health care information management utilizing Cloud Computing and Android OS. In*Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE* (pp. 1037-1040). IEEE.

Embi, P. J. (2001). Information at hand: using handheld computers in medicine.*Cleveland Clinic Journal of Medicine*, *68*(10), 840-842.

Encyclopedia Britannica. (2013). Moore's Law. Retrieved from http://www.britannica.com/EBchecked/topic/705881/Moores-law

European Commission. (2014). Protecton of Personal Data. Retrieved from http://ec.europa.eu/justice/data-protection/

Fernandez-Alemán, J. L. F., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in EHR: A systematic literature review. *Journal of biomedical Informatics*.46, 541-562.

Financier Worldwide. (2012). Data Protection & Privacy Laws. Retrieved from http://www.financierworldwide.com/AnnualReviews/AR_DataProtection_326jpm.pdf.

Fischer, S., Stewart, T. E., Mehta, S., Wax, R., & Lapinsky, S. E. (2003). Handheld computing in medicine. *Journal of the American Medical Informatics Association*, *10*(2), 139-149.

Global Research (2013). Canada Spied on Brazil's Government as Part of Global Commercial Espionage Campaign. Retrieved from http://www.globalresearch.ca/canada-spied-on-brazils-government-as-part-of-global-commercial-espionage-campaign/5353642

Government of Canada. (2013). An Overview of the Canadian Charter of Rights and Freedoms. Retrived from http://www.pch.gc.ca/eng/1355760105725/1355760725223

Government Nova Scotia. (2013). Personal Health Information Act. Retrieved from http://novascotia.ca/dhw/phia/public.asp.

Hung, P. C., Andrade, J., Chen, Y., Huang, R., Martin, M. V., & Zheng, Y. (2007, May). Research issues of privacy access control model for mobile ad hoc health care applications with xacml. In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on* (Vol. 2, pp. 582-587). IEEE.

Hunton & Williams (2013). Brazil Moves Forward with Internet and Data Protection Bills. Retrieved from https://www.huntonprivacyblog.com/2013/11/articles/brazil-moves-forward-Internet-data-protection-bills/.

Kalra, D. (2006). EHR standards. *Yearb Med Inform*, 136-144.

Kerr, I., & Caulfield, T. (2008). Emerging health technologies. *Canadian Health Law and Policy*, 509-538.

Kosseim, P., & El Emam, K. (2009). Privacy interests in prescription data, part I: Prescriber privacy. *Security & Privacy, IEEE*, *7*(1), 72-76.

Lapinsky, S. E., Weshler, J., Mehta, S., Varkul, M., Hallett, D., & Stewart, T. E. (2001). Handheld computers in critical care. *CRITICAL CARE*-LONDON, 5(4), 227-231.

Lasprogata, G., King, N. J., & Pillay, S. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stan. Tech. L. Rev.*, *2004*, 4, 1-50.

Levin, A., & Nicholson, M. J. (2005). Privacy law in the United States, the EU and Canada: the allure of the middle ground. *U. OTTAWA L. & TECH. J.*, *2*, 357-395.

Liu, W., & Park, E. K. (2013). e-Health care Cloud-Enabling Characteristics, Challenges and Adaptation Solutions. *Journal of Communications*, *8*(10). 612-619.

Microsoft. (2014). Hash and Signature Algorythms. Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/aa382459%28v=vs.85%29.aspx

McCaffery, J.MSDN Magazine. (2003). Keep Your Data Secure with the New Advanced Encryption Standard. Retrieved from http://msdn.microsoft.com/en-us/magazine/cc164055.aspx

Miller, R. H., West, C., Brown, T. M., Sim, I., & Ganchoff, C. (2005). The value of electronic health records in solo or small group practices. *Health Affairs*,*24*(5), 1127-1137.

Mizukami, P.N, Moncau, L.F. (2014). Brazilian Chamber of Deputies Approves Marco Civil Bill. Retrieved from http://infojustice.org/archives/32527

National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing. Retrieved From http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Nisker, J. (2006). PIPEDA: A Constitutional Analysis. *Canadian Bar Review*, *85*, 317-343.

Nkosi, M. T., & Mekuria, F. (2010, November). Cloud computing for enhanced mobile health applications. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on* (pp. 629-633). IEEE.

Novais, A. (2012). Health care in Brazil. The Brazil Business. Retrieved from www.http://thebrazilbusiness.com/article/healthcare-in-brazil

Office of the Privacy Commissioner of Canada. (2008). Privacy Breaches. Retrieved from https://www.priv.gc.ca/resource/pb-avp/pb-avp_intro_e.asp

Office of the Privacy Commissioner of Canada. (2013). New privacy challenges demand stronger protections for Canadians. Retrieved from https://www.priv.gc.ca/media/nr-c/2013/nr-c_130523_e.asp

Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2012). Design and implementation of a cloud based rural health care information system model.*Univers J Appl Comput Sci Technol*, *2*(1), 149-157.

Paim, J., Travassos, C., Almeida, C., Bahia, L., & Macinko, J. (2011). The Brazilian health system: history, advances, and challenges. *The Lancet*, *377*(9779), 1778-1797.

Peyton, L., Hu, J., Doshi, C., & Seguin, P. (2007, July). Addressing privacy in a federated identity management network for ehealth. In *Management of eBusiness, 2007. WCMeB 2007. Eighth World Congress on the* (pp. 12-12). IEEE.

Presidency of the Republic (2007). Law No. 8078 OF 11 September 1990. Retrieved from http://www.planalto.gov.br/ccivil_03/leis/l8078.htm

Privacy Laws & Business. (2014). Brazil issues fine of 1.2 million euros under new Internet privacy Law. Retrieved from http://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/8/Brazil-issues-fine-of-12-million-euros-under-new-Internet-privacy-law/

Prokopieva, E. (2005). New Federal and Provincial Personal Information Protection Legislation and its Impact on Physicians and Public Hospitals.*Canadian Journal of Law and Technology*, *4*, 45-57.

Rolim, C. O., Koch, F. L., Westphall, C. B., Werner, J., Fracalossi, A., & Salvador, G. S. (2010, February). A cloud computing solution for patient's data collection in health care institutions. In *eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED'10. Second International Conference on* (pp. 95-99). IEEE.

Samsuri, S., Ismail, Z., & Ahmad, R. (2010). Towards implementing a privacy policy: An observation on existing practices in Hospital Information System.*Journal of e-health Management*, *2011*, 1-9.

Schwartz, P. M., & Solove, D. J. (2011). PII Problem: Privacy and a New Concept of Personally Identifiable Information, The. *NYUL Rev.*, *86*, 1814-1894.

Scott, R. E., Jennett, P., & Yeo, M. (2004). Access and authorisation in a Glocal e-Health Policy context. *International journal of medical informatics*,*73*(3), 259-266.

Sparks, M. (2014). FIDO. New log-in tech will make passwords obsolete. Retrieved from http://www.independent.ie/business/technology/news/fido-new-login-tech-will-make-passwords-obsolete-30817739.html

ThomsonReuters. (2012). Data Protection in Brazil: Overview. Retrieved from http://uk.practicallaw.com/4-520-1732.

Varshney, U. (2007). Pervasive health care and wireless health monitoring.*Mobile Networks and Applications*, *12*(2-3), 113-127.

West, D. (2012). How mobile devices are transforming health care. *Issues in Technology Innovation*, *18*, 1-14.

Webster, P. C. (2011). The rise of open-source EHR. *Lancet*, 377(9778), 1641-1642.

Webster, I., Ivanova, V., & Cysneiros, L. M. (2005). Reusable Knowledge for Achieving Privacy: A Canadian Health Information Technologies Perspective.*WER*, *5*, 112-122.

Win, K. T. (2005). A review of security of EHR. *Health Information Management*, *34*(1), 13-18.

Wollersheim, D., Sari, A., & Rahayu, W. (2009). Archetype-based EHR: a literature review and evaluation of their applicability to health data interoperability and access. *HIM J*, *38*(7), 7-17.

World Health Organization. (2006). Brazil. Retrieved from http://www.who.int/goe/data/country_report/bra.pdf.

Zoutman, D. E., Ford, B. D., & Bassili, A. R. (2004). The confidentiality of patient and physician information in pharmacy prescription records. *Canadian Medical Association Journal*, *170*(5), 815-816.