**By Sommer Abdel-Fattah, McMaster University**

**Student # 0242088**

**Master's Engineering and Public Policy Degree Conferred December 2008, current PhD student**

# Privacy and Security of Medical Hospital Records

**Communications Technology Policy Solutions**

**Sommer Abdel-Fattah**

**59 Larraine Ave.**

**Dundas, Ontario**

**L9H 6E5**

**abdelfs@mcmaster.ca**

**905-317-9098**

# Table of Contents

**Abstract**

The push toward electronic medical records has been coupled with a concern for privacy, security, trust and confidentiality. Increasing the problem is the lack of strict data sharing and protection laws governing the healthcare industry. Investigating the current regulations regarding privacy and security in Ontario will be important in recommending the important qualities of a communication data base system for medical records. These insights will also provide insight into the development a policy suggestion for improvement of privacy and security of medical records.

**Introduction**

Development of electronically linked patient records or Electronic Health Record schemes (EHRs) are a priority item for governments in many countries, including Canada, as part of a vision for future health care services. The model is likely to include using web-based patient information and tele-health. This article discusses the privacy framework needed for secure patient medical records. This paper aims to review the privacy frameworks in Canada including the underlying provincial regulations. This paper will work to develop suggestions for a medical record system that will encompass the provincial standards as well as help to combat privacy and security issues of patient medical records (Cornwall, 2002).

EHRs offer health care providers access to a more complete medical history of a patient, with the patient's consent. They are generally used in conjunction with 'decision support' software systems for health professionals, providing medical information such as clinical guidelines and checks. EHRs therefore promise to improve the quality of health care services, promote a more integrated approach to care and offer consumers an opportunity to better manage their own

health care. EHRs have been designed to perform a number of different functions. Current EHR schemes are primarily for financial purposes, such as processing claims for health insurance and government health benefits (Cornwall, 2002).

The need for addressing health record privacy is becoming increasingly critical for the following reasons:

- Extreme sensitivity for personal health information
- Patchwork of rules across the health sector
- Increasing electronic mode of health records and exchange of data electronically
- Multiple levels of providers and integration of services
- Development of health networks
- The growing emphasis on improved use of technology and computerized records

France, Germany, England and Ireland have had data protection laws for almost 25 years, although their jurisdiction has been limited to the public sector, until recently. The laws varied widely until common privacy and data protection requirements were developed by the European Union (EU) under the EC *Data Protection Directive*. The Directive establishes common elements of privacy and data protection laws that must be adopted by member states. France, Germany, Ireland and England fully implemented the Directive in 2001 and 2002 (Cornwall, 2002). Similarly, the SESAM Vitale system in France has operated nationally since 1998 to provide secure electronic processing of insurance claims for all the population. It is comprised of a consumer held smart card (Vitale card), a card for health professionals and a social health network that provides information to health professionals. The smart cards restrict access to the system, ensuring that patient records can only be accessed when the consumer is present. The

social health network uses Intranet technology for secure mail exchange, an index of all registered users, electronic address book, transmission of health care forms, medical news, databases, some medical education information, sanitary alerts and diagnostic and prescription advice (Cornwall, 2002).

In Canada, the regulation of privacy in the health sector is a provincial responsibility. Each province and territory has privacy laws covering public agencies, but many of these until recently did not cover health service providers such as hospitals. The Canadian government provided an incentive for provinces to introduce privacy and data protection laws, initially for the private sector with the Personal Information Protection and Electronic Documents Act 2001. Initially the law applied only to private enterprises that come under federal jurisdiction. Canadian Health Ministers have agreed to a harmonized privacy framework in the health sector (Cornwall, 2002).

In Canada, health information networks are being developed in every province to enhance patient care and manage an increasingly complex health care system. Researchers and policy-makers are trying to establish common community level indicators of health to be linked with healthcare and social services utilization data. The British Columbia Pharma*Net* system, introduced in 1995, provides online, realtime processing of a range of entitlements and benefits for British Columbian residents (Cornwall, 2002). Pharma*Net* provides pharmacists with a province-wide patient medication history, comprehensive drug information and automatic checks such as drug interactions. It has also been available in hospital emergency rooms for some years (Cornwall, 2002). The Pharmaceutical Information Network (PIN) in Alberta covers medicines information

held by doctors, hospitals and pharmacists. PIN is part of Alberta's Wellnet scheme, which aims to provide an umbrella for provincial and regional initiatives to build an integrated health information network (Cornwall, 2002).

In Ontario, one of the earliest initiatives was the ePhysician Project to develop a secure intranet for general practitioners who have agreed to be part of Primary Care Networks to access each other's patient records, with the patient's consent (Cornwall, 2002). It is part of Smart Systems for Health (SSH), an initiative of the Ontario Ministry of Health and Long Term Care that provides the infrastructure for secure communication of patient information among health care providers across the province (Cornwall, 2002).

Due to the individual provincial systems, the Canadian government has promoted a collaborative approach to EHR development to promote interoperability. A Canada wide Health Infostructure Plan was released by Canadian Health Ministers in 2001. Canada Health established the Office of Health and the Information Highway (OHIH) to provide project leadership and funding for government health infostructure programs. OHIH invested $80 million in a two year Partnership Program to support national implementation of information and communications (Cornwall, 2002). This article examines techniques to meet privacy and security goals through well designed database communication systems.

**Background**

Many jurisdictions have enacted or are developing legislation to protect the privacy of personal information, and personal health information in particular, and the confidentiality and security of such information. On January 1, 2004, the federal Personal Information Protection and

Electronic Documents Act (PIPEDA) began to apply throughout Canada to organizations when they collect, use or disclose personal information in the course of "commercial activities", except in areas in which provinces have enacted legislation deemed by the federal Cabinet to be "substantially similar." This includes commercial activities in the business, health and not-for-profit sectors (MOH, 2004). PIPEDA has been identified by health sector stakeholders as especially problematic for organizations that collect, use or disclose personal health information for health care purposes, since it was not developed with the special needs of health care in mind MOH, 2004).

The Personal Health Information Protection Act, 2004 ("PHIPA") is designed to address these concerns and to achieve the purposes set out in the Act. The Personal Health Information Protection Act, 2004 is the culmination of ongoing efforts over a number of years to develop appropriate legislative provisions for Ontario to ensure the privacy of personal heath information in a manner that would be consistent with the effective provision of health care (MOH, 2004). Bill 31 (Health Information Protection Act, 2004), consists of the Personal Health Information Protection Act, 2004 (Schedule A) and the Quality of Care Information Protection Act, 2004 (Schedule B). The Bill received Royal Assent on May 20, 2004 and came into force on November 1, 2004 (MOH, 2004).

**The Personal Health Information Protection Act (PHIPA)**

On November 1, 2004, the Personal Health Information Protection Act (PHIPA) came into effect. The new law sets out the rules that healthcare providers or "health information

custodians" must abide by when collecting, using, and sharing personal health information and gives patients the right to access to their health records and correct any mistakes (PHIPA, 2004).

The purpose of PHIPA is to establish rules for the collection, use of disclosure of personal health information and the privacy of individuals with respect to that information, while facilitating effective healthcare (MOH, 2004).

In this act, personal health information means identifying information about an individual relating to the physical or mental health of the individual, including family history, details of the provisions of health, their healthcare provider, their payments or eligibility for coverage of healthcare, donation of organs, health number or any health examination results information (PHIPA, 2004).

PHIPA applies to individuals and organizations involved in the delivery of healthcare services, including and not limited to hospitals. The hospital, including doctors, nurses, physiotherapists, chiropractors, massage therapists, dietitians and other healthcare providers are defined as health information custodians by the Act. Under PHIPA, they are required to

• collect only the information they need to do their job

• take steps to safeguard your personal health information

• take reasonable steps to ensure your health records are accurate and complete for the work they do

• provide a written description of the practices they use to protect your information, and the name of the person to contact if you have any questions or concerns about your personal health records.

Under PHIPA, patients have the right to consent to how their information will be collected, used and shared, except in specific circumstances where the law authorizes healthcare providers to collect, use or share a person's information without consent, such as reporting for public health safety. The act specifies two types of consent; implied consent and express consent. Implied consent states that the healthcare provider will assume consent for the sharing of health information to provide healthcare to the patient without directly asking or requiring a signature for consent. For example, when a family physician refers a patient to a specialist, he or she will assume that permission is given to share the preexisting health information with the specialist unless the patient specifically refuses. In practice, PHIPA permits the healthcare providers to assume implied consent to collect, use or disclose health information with other healthcare providers who are involved in the patients care unless they state otherwise. Express consent applies that a healthcare provider is required to request patient consent either orally, in writing or electronically before sharing health information (PHIPA, 2004). For example, if a healthcare provider is asked to disclose personal health information to someone who is not a health information custodian under PHIPA, like an employer, he or she must obtain express consent (MOH, 2004).

Another application of PHIPHA is the patients' ability to access their personal health records. In order to access personal records, a request in writing, is sent in and the health information custodian has 30 days to respond to the request but, in certain situations, may require an extension of up to 30 days. Under PHIPA¸ health information custodians can only deny access to record of personal health information in certain situations, such as when health information was collected as part of an investigation, and an explanation must be provided.  These decisions can

be appealed by contacting the Information and Privacy Commissioner of Ontario. If personal records are thought to be inaccurate or incomplete, requests can be made to have changes made.

The Act explicitly stipulates the importance of security; “a health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian’s custody or control is protected against theft, loss, and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal” (PHIPA, 2004). Thus it is clear that privacy and security of health records is important in protecting patient rights.

**Medical Records Database**

The development of electronic medical records needs to include two important elements: that record systems should be designed so that they can exchange all their stored data according to public standards and, secondly, that patients should have control over access and permissions (Mandl, 2001). Building software compliant with public standards will enable connectivity of diverse systems. It may also be important to allow patients' control over their own protection of privacy according to individual preferences and help prevent some of the current misuses of personal medical information. The purpose behind these doctrines is to ensure long term access of patients and care providers to medical records for clinical use while minimizing the risk to privacy (Mandl, 2001).

Open standards should be used in the exchange of information among different systems; for example, developing a voluntary consensus database of electronic data exchange in healthcare environments. The system would be compatible for sending or receiving data on patient admissions, registration, discharge, or clinical observations, and billing (Mandl, 2001).

For different systems to share data effectively they must use a common set of communication protocols and formats to allow the import and export of their data. Common data structures and open source programming can foster the possibility of effective data exchange among systems.

The fact that patients have trouble accessing their medical information while that very information has exacerbated worries about the confidentiality and proper use of that record. A particular concern about online medical data is that companies providing the record software or maintaining the record systems want to own the patients' data (Mandl, 2001). Giving patients control over permission to view their record, as well as over its creation, collation, annotation, modification, dissemination, use, and deletion is key to ensuring patients' access to their own medical information while protecting their privacy.

A patient's medical records are generally fragmented across multiple treatment sites, posing an obstacle to clinical care, research, and public health efforts. Electronic medical records and the internet provide a technical infrastructure on which to build longitudinal medical records that can be integrated across sites of care. However, the choices about the structure and ownership of these records will have a profound impact on the accessibility and privacy of patient information. Already, alarming risks are apparent as proprietary online medical record systems are developed and deployed. The technology promising to unify the currently disparate pieces of a patient's medical record may actually threaten the accessibility of the information and compromise patients' privacy. Mandl's 2001 article "Public standards and patients' control: how to keep electronic medical records accessible but private," describes six desirable characteristics to guide the development of online medical record systems, listed below.

● **Comprehensiveness-** Outpatient records should contain, problem lists, procedures, allergies, medications, immunizations, history of visits, family medical history, test results, doctors' and nursing notes, referral and discharge summaries, patient-provider communications, and patient directives. The records must also span a lifetime, so that a patient's medical and treatment history is available as a baseline and for retrospective analysis.

● **Accessibility-** records should be universally available, such as on the world wide web. This is vital to patient access to better care in emergency cases worldwide.

● **Interoperability-** different computerized medical systems should be able to share records. Data should be compatible to be able to transfer historical, radiological, laboratory, etc from multiple sources, including doctors' offices, hospital computer systems, laboratories, and patients' personal computers. Without interoperability, even electronic medical records will remain fragmented.

● **Confidentiality-** patients should have the right to decide who can examine and alter what part of their medical records. A patient might choose to allow no access to such records, though at the risk of receiving uninformed and thus inferior care. At the other extreme some may make their records completely public. For most patients, the appropriate degree of confidentiality will fall in between and will be a compromise between privacy and the desire to receive informed help from medical practitioners. Because an individual may have different preferences about different aspects of his or her medical history, access to various parts of the record should be authorized independently.

● **Accountability-**any access to or modification of a patient's record should be recorded and visible to the patient. Thus, data and judgments entered into the record must be identifiable by their source. Patients should be able to annotate and challenge their records, though they should not be able to delete or alter information entered by others. Patients should also be able to see who has accessed any parts of their record, under what circumstances, and for what purpose. Reliable authentication is essential to make this feasible. Appropriate laws can reinforce accountability built into the records system.

● **Flexibility-** most want to make data about themselves available to those trying to improve medical knowledge, the practice of medicine, and the education of the next generation of healthcare providers. This altruism has limits, however, when patients feel the threat of exploitation, the risk to privacy, or unsolicited follow up contacts. Patients should thus be able to grant or deny access to selected personal medical data. This can be based on personal policies or decisions about specific studies.

Despite what may seem to be clear cut strategies for improving privacy and security of patient records, technology applications must be considered for a more holistic solution.

**Technology Solutions**

Information and communications technologies (ICTs) are transforming the world through revolutionary developments in bandwidth, storage, processing, mobility, wireless and networking technologies (Carter, 2008). The health-care sector has recognized the value of new technologies for improving privacy and security (Carter, 2008).

The future of the healthcare sector is moving towards a wireless environment. This will attempt to minimize the paper trail of patient files and allow for instant recall of patient records and identification information.

Healthcare providers around the world are recognizing the benefits of adopting Radio Frequency Identification (RFID) technology into their operations, in order to enhance health care service delivery. RFID is a contactless technology that uses radiofrequency signals to transmit and receive data wirelessly from RFID tags or transponders to RFID readers (Carter, 2008). RFID information can capture time and location data upon which item histories and profiles can be constructed (Carter, 2008).

The advantage of using this kind of RFID for healthcare delivery include:

- Accurate identification without the need to touch the RFID tag
- Sensors can be incorporated into RFID tags to identify position
- Data stored inside RFID tags can be encrypted, modified and rewritten
- Tags are recyclable and can be made difficult to counterfeit
- Special devices are required to read RFID tags, increasing privacy

(Carter, 2008)

RFID is expected to increase patient privacy and security by using RFID-enabled identification bracelets for newborns and patients (Carter, 2008). This means that patients can be positively identified, prescribing and checking drug interactions at the point of care, quickly checking a patient's blood type, matching newborn invents with their parents and triggering a lock-down after the unauthorized removal of an infant from a secured area. Thus, RFID can help to improve patient registration and management process (Carter, 2008).

Regarding security, there are concerns that RFID tags are susceptible to many of the same data security issues associated with any wireless device, including interception, hacking, and cloning. There are solutions to combat these issues, such as shielding, tag encryption, reader authentication, role-based access control, and the addition of passwords.

The privacy of the information contained within the RFID technology would certainly be another important component to consider. The RFID database would link the identity of the patient with their health information. Thus, measures would need to be taken to develop measures against theft or loss of handheld devices, prevent unauthorized use and disclosure, strong security around retention, transfer and disposal, as well as stronger, more accountable governance mechanisms to trace users (Carter, 2008).

Pilot projects are currently underway in Canada. Hamilton Health Sciences launched a multi-phased multi-year RFID initiative to explore and assist in development of better business tools for healthcare (Carter, 2008). The initial efforts focused on exploring the economic and technical feasibility. Expected efficiency benefits include labour savings, reduced hospital (Carter, 2008).

There are however some issues to be considered with RFID implementation. The cost of the technologies initially will be high, as tags and readers will need to be purchased; consulting, operational process design and staff training will increase current cost. However as the RFID technology is re-useable, and once training is complete, costs are expected to decrease (Carter, 2008). There is also more information needed on accommodating the integration of RFID with current hospital database information with new RFID technology. Also, more testing needs to be done on the reliability of the system within the hospital environment with the interaction of current machines such as heart monitors (Carter, 2008).

RFID implementation will need to be highly customized to support the business processes they automate to be specific to the medical record system used at the specific hospital.

One hospital in New Jersey, specialized in acute care, has already implemented RFID for managing patient files. Seeking increased efficiency and compliance with PHIPA, each patient file is tagged with an RFID tag, allowing it to be tracked from the moment it is created until the file is retained for storage. RFID readers are positioned in key locations around the centre to enable automatic tracking and encoding of the tags as they are moved from one place to another. Reads and writes to the tag are dynamically updated in the central database, ensuring real-time, accurate location data (Carter, 2008). The centres also have a series of handheld readers for routine inventory and locating misplaced files (Carter, 2008).

Under PHIPA, suppliers of electronic services that enable health information custodians to collect, use, modify, disclose, retain or dispose of personal health information are bound to obligations. These include not using personal health information except as necessary in the course of providing services, not disclosing personal health information, and not permitting employees or others acting on the suppliers behalf to have access to personal health information unless they agree to be bound by these restrictions (Carter, 2008).

Despite the advancements in technology applications to protect privacy and security, there are still some current logistical challenges.

**Challenges**

There are important challenges in implementing personally controlled systems on a large scale. No matter how well these are integrated with institutional information systems, it is unlikely that patient controlled records could entirely replace provider or hospital based records. For

important clinical and financial reasons, providers need control over their own version of patients' medical histories. Also, it is possible that patients may self-diagnose, or self-prescribe treatments due to findings on their own records. However, it is possible that portions of the personally controlled records would be downloaded into the institutional record to complement the existing data (Mandl, 2001).

Another issue is hackers. No matter how sophisticated security systems become, people always manage to defeat them. This could lead to the problem of exploitation of human weakness to subvert someone with legitimate access to the data. Fortunately, technical advances in security systems for electronic records should continue to be driven forward by the commercial interests of companies doing business over the internet.

A problem that is often overlooked is the fact that No computer system has ever remained operational for the lifetime of a typical person; hence we will need procedures to migrate records to new computer systems and architectures (Mandl, 2001). This brings up another issue of the need to develop acceptable procedures for backing up data, anticipating recovery in case of disasters, agreeing on whether emergency overrides of patient's policies are ever acceptable, whether it is possible to retract access to data once it has been given, who is trusted to conduct audits (Mandl, 2001).

It is unlikely that one single institution can hope to encompass a patient's entire record. Ideally, it should be possible to create or assemble each patient's personal health record so that it is accessible at all points of care within the health service and contains data from all institutions involved in that patient's care. Two main impediments stand in the way of this ideal. Firstly, most healthcare institutions show little willingness to share data with their competitors.

Secondly, patients are becoming increasingly anxious about the privacy of their medical records. Such concerns seem justified when one considers that, under current laws and practices, identifiable medical data are routinely shared with insurance companies, government, researchers, employers, local retail pharmacies, attorneys, and others (Mandl, 2001).

The widespread adoption of patient controlled health records proposed will depend on solutions being found to these challenging technical and policy issues.

**Policy Suggestions**

Noting the challenges above, some of these issues may be solved through policy development. Considerable further evolution of accepted policies and laws so that patients are not coerced into signing away their privacy rights to obtain care or reimbursement will be an important first policy step to build trust and accountability. Also, due to the fact that care is normally provided to a patient by different doctors, nurses, pharmacists, and other providers, and, with the passage of time, by different institutions in different geographical areas, each provider must be able to know what others are currently doing and what has previously been done. Patients should also be able to see who has accessed any parts of their record, under what circumstances, and for what purpose. Reliable authentication is essential to make this feasible. This could be a policy statement that all medical entries be date stamped electronically with names of those inputting the data or accessing the record. Appropriate laws can reinforce accountability built into the records system. Patients should thus be able to grant or deny access to selected personal medical data. An example policy might state that any study may use data if they will be stored only in an aggregated, non-identifiable form. Patients should also have the right to agree to more intrusive

participation in specific studies. Whether patients are willing to be solicited on the basis of characteristics of their record should also be controllable. Patients could provide time limited keys to other parties to access a specified segment of their record. For example, they could permit hospitals to write to (but not read) the laboratory results section of their record.

Conflicting views on the shape of standard records have caused some stagnation in the development of effective health record database systems. Some anticipate records consisting of a collection of web documents, whereas others emphasize the importance of coded structured data that can be retrieved for aggregation, analysis, and decision support (Mandl, 2007). The challenge is to build on the strengths of both approaches to develop record systems that are useful as well as user friendly. These systems should have the attributes identified.

Privacy rights, as such, should be further defined in policy to be the right to control the circulation of personal information about oneself, freedom from unreasonable interference in one's private life and the right to protect personal data against misuse or unjustified publication.

**Applications**

Privacy and security in healthcare brings up another important emerging issue to address. Genetic information and the ethics, privacy and security issues embedded within have surfaced as a controversial topic. The field of genetic engineering has become more complicated with the finding that it is now possible to identify individuals using genetic markers to predict if that person will have particular genetic diseases. The concern now is about what types of genetic testing are necessary, who should have access to this information once testing is complete and how that information should be used (Collins, 2001). One of the great benefits of genetics has

been the ability to uniquely identify individuals, however, whenever such information is stored, the issue of security becomes heightened. Databases must be secured and only authorized individuals should have access to the data. The other issue is whether the patient themselves should have access to this data. If it is placed in their accessible medical history, patients may find out information they may not want to know. Alternatively, it could be used by other sources, such as insurance agencies which may deny insurance based on genetic predeterminations. The problems associated with genetic information security being compromised and accessed by an unauthorized source are frightening.

**Conclusion**

Privacy and security of medical records is underpinned by two principles: the need for public standards and the need to respect patients' right to privacy. These issues are at the heart of any coherent approach to electronic patient records. It is thus important to develop public standards for health communication. Designing an electronic medical record system should include a way to exchange all stored data according to public standards. These public standards include giving patients control over permissions to view their record as well as creation, collation, annotation, modification, dissemination, use, and deletion of the record while protecting their privacy. Many existing electronic medical record systems fragment medical records by adopting incompatible means of acquiring, processing, storing, and communicating data. Record systems should be able to accept data from multiple sources. In order to enhance privacy and security through these mechanisms, it will be important to include policy changes to makes these integral components of the healthcare sector.

The foundations are in place for standards on which to base communication of electronic records. Computerized medical information systems are at the start of what promises to be a rapid evolution.

**References**


1. Cornwall, Amanda (2002). *Electronic Health Records: An International Perspective.* Health Issues, Number 73, pp. 19-23.

2. Ministry of Health and Long term care (2004). Personal Health Information Protection Act: An Overview for Health Information Custodians.
3. RC Barrows, RD Clayton (1996). Privacy, confidentiality, and electronic medical records. Journal of the American Medical Informatics Association, Vol 3, American Medical Informatics Association, New York,139-148.
4. Mandl KD, Simons WW, Crawford WC, Abbett JM. Indivo: a personally controlled health record for health information exchange and communication BMC Med Inform Decis Mak 2007;7:(1):25Sep 12. [PubMed].
5. Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private BMJ 2001;322:(7281):283-287Feb 3. [PubMed].
6. Text of the Personal Health Information Protection Act, 2004:

   http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm

   http://www.ontla.on.ca/documents/Bills/38_Parliament/Session1/b031ra.pdf

7. Text of the Minister's notice of the proposed regulations for public consultation:

   http://www.ontariogazette.gov.on.ca/mbs/Gazette/Gazette.nsf/Main/C55931AF70373F0085256EC5006931F3/$FILE/137-27.pdf

8. Legislative history of Personal Health Information Protection Act, 2004:

   http://www.ontla.on.ca/documents/Bills/38_Parliament/Session1/index.htm#P288_21637

9. Related Ministry of Health and Long-Term Care documents:

   Http://www.health.gov.on.ca/english/public/updates/archives/hu_03/priv_legislation.html

   http://www.health.gov.on.ca/english/providers/project/priv_legislation/priv_legislation.html

10. Carter, Fred. RFID and Privacy: Guidance for Health-Care Providers (January 2008). Information and Privacy Commissioner of Ontario.