Health Information and Privacy Impact Assessments

Internship Report
IWK Health Centre

Submitted by:

David Hancock
Banner ID: B00426486

April 14, 2006

In partial fulfillment of the requirements of the Master of Health Informatics Program, Dalhousie University

Executive Summary

The Romanow Report recommends that “Canadians should have ownership over their personal health information, ready access to their personal health records, clear protection of the privacy of their health records, and better access to comprehensive and credible information about health, health care and the health system”. Privacy is an individual right to control the circulation of personal information. Confidentiality is the obligation of a person or organization to protect personal information. Health providers, information managers, health informaticians and others are the custodians of personal health information entrusted to them by the most vulnerable of the population, those that are seeking medical services. They are duty-bound to respect the individual’s privacy rights. Proper management of this personal health information is essential to maintain the confidentiality and prevent the misuse or unjustified use of this sensitive information. The need to protect the privacy of health information has never been greater. Increasingly the need exist for the flow and exchange of personal health information through the use of technology including electronic patient records. So how are health information custodians ensuring that they are meeting the obligation to protect this sensitive information? The current privacy laws in Canada are made up of patchwork of legislations. There are rules for the private sector and the public sector. How is this information going to flow across the federal, provincial and territorial jurisdictions? These are all very important questions. These important subjects are discussed in this internship report however; the focus is on the early detection of privacy problems. The key subject is the use of Privacy Impact Assessments (PIA). A PIA is a front line privacy defense tool which is also valuable for identifying privacy risk and documentating mitigation strategies. It provides a methodology for ensuring this sensitive information is protected and should be used on all systems which collect, use or disclose personal information.

Acknowledgement and Endorsement

This internship report has been written by David Hancock in partial fulfillment of the requirements for the Master of Health Informatics Program at Dalhousie University. This report has not received any previous academic credit at Dalhousie University or any other institution.

I would like to thank Valerie Shaffner and Ken George of the IWK Health Centre for allowing me to participate in this initiative. I would also like to thank Greg Lapowy, Health Informatics graduate 2006, and Michelle Guignac from the Nova Scotia Department of Health Information, Access & Privacy Unit for sharing their knowledge of privacy impact assessments in health. I would like to acknowledge Rick Stewart, Technology Assessment Officer, IWK Health Centre for listening to my challenging issues and providing advice and guidance during this project.

David Hancock

Table of Contents

1. Introduction

Health care systems are complex enterprises with multiple stakeholders requiring access to a variety of health information. The collection and use of personal health information stored in these systems is a concern shared by many Canadians. When personal health information is being collected, used, disclosed, stored or secured it must comply with a variety legislative requirements. Health Informatics professionals should therefore have an understanding of privacy law, privacy design and the role of Privacy Impact Assessments (PIA) as a process to ensure compliance with relevant statutory requirements. Failure to achieve adequate protection of health information collected increases the risk of health care organizations to the misuse or unjustified use of sensitive information. This report focuses on the issues of privacy, confidentiality and security of personal health information.

A Privacy Impact Assessment is a risk assessment tool used by decision makers to ensure information systems, programs and policies meet basic privacy requirements. It measures both the technical compliance and the broader privacy implications such as ethical and moral issues. This report serves as a guide to understand how the collection, use, sharing and disclosure of personal information can be affected by privacy legislation and privacy standards of practice. It presents a methodology for conducting Privacy Impact Assessments as a tool to promote fully informed policy making choices.

The research and work carried out in support of this internship includes developing a Privacy Impact Assessment tool for personal health information, and technology assessment and evaluation of patient monitoring systems intended for use in the Neonatal and Pediatric Intensive Care areas of the IWK Health Centre.

2. IWK Health Centre

Located in Halifax, Nova Scotia, the IWK Health Centre provides quality care to children, youth, women and families in the three Maritime Provinces and beyond. Each year, there are approximately 5,000 babies delivered at the IWK. Maritime children, women, youth and newborns spend approximately 260,000 days as inpatients or in clinics at the Health Centre. The IWK has 101 adult beds, 110 for babies and 121 beds for children. The IWK is structured around a Program-Based Care Model that puts people first by organizing interdisciplinary care teams around the needs of patients and families. Through Program-Based Care, the IWK's administrative structure emphasizes shared responsibility among health care workers to deliver care with a patient/family-oriented approach. Services provided by the Health Centre are delivered through three programs: Children's Health; Child and Adolescent Mental Health; and Women's and Newborn Health.

2.1 Quality Resources & Decision Support Services

The Quality Resources and Decision Support Services Team (QRDSS) has a leadership role at the IWK and is responsibility for a number of centre wide services related to Quality, Risk and Decision Support.

QRDSS Areas of Responsibility

- ✓ **Quality Leadership**
- ✓ **Quality Planning and Improvement**
- ✓ **Patient Safety**
- ✓ **Risk Management**
- ✓ **Decision Support Services**
- ✓ **Privacy and Confidentiality**

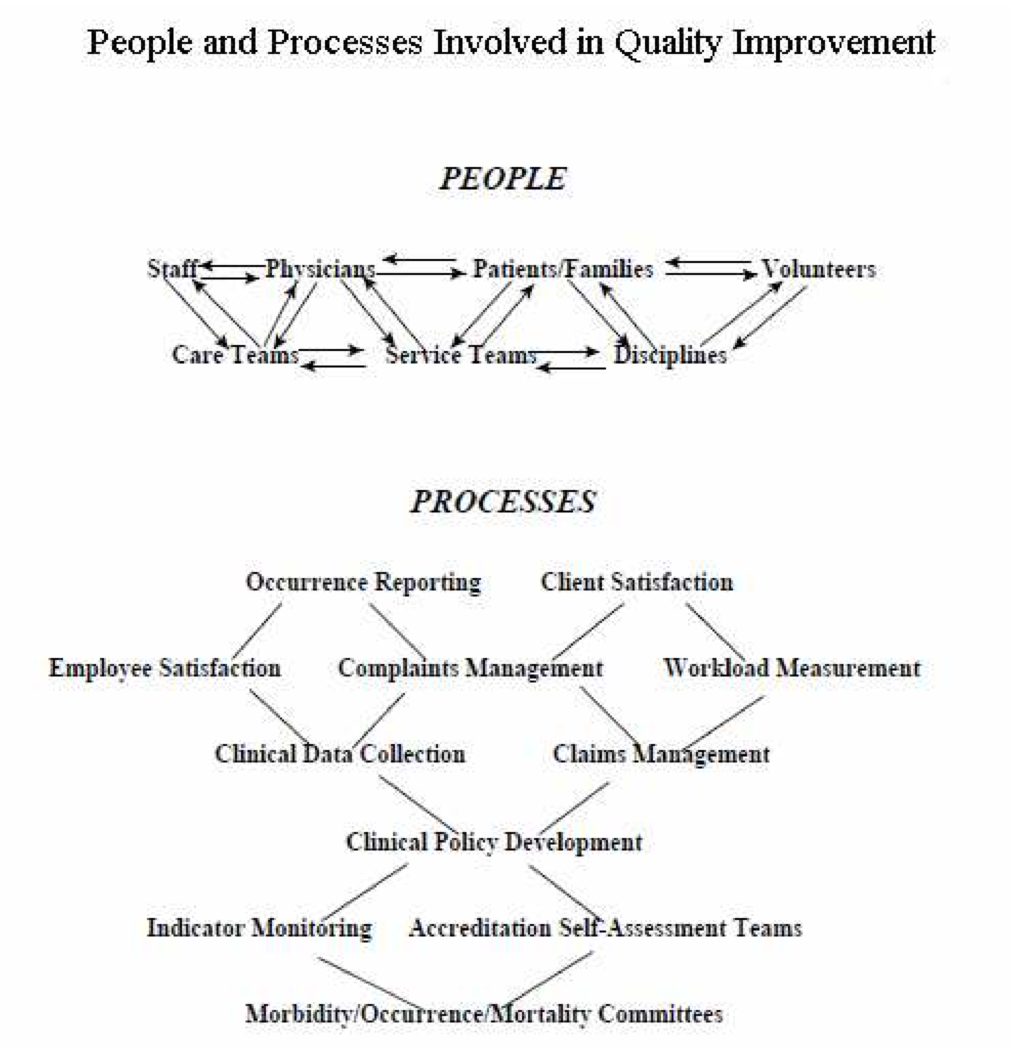


Figure 1: QRDSS People and Processes

Figure 1 demonstrates the various interactions of the QRDSS with people and processes, both internally and externally, in the provision of information that assists with decision-making.

Quarterly reports including Team Report Cards, Opinion Survey Data, Unusual Occurrence Reports, Workload Measurement Data, Clinical Data and Report Card Data are provide to health care teams.

3. Internship Role and Work Performed

The internship position was created as the result of a meeting with the QRDSS and the Biomedical Engineering unit of the IWK Health Centre in early 2005. The subject of the meeting was the impact new privacy legislation in both the United States and Canada would have on the collection, storage and use of health information in clinical information systems. It was recognized that PIA's in the near future would be a mandatory requirement for assessing the risks of all systems and practices that collect, use and disclose personal health information. The result of the meeting was the creation of an internship position for a Health Informatics student with a background in both clinical systems and information technology. It was identified as a priority within QRDSS and would be a proactive measure to move forward with a PIA process.

3.1 Scope of Internship

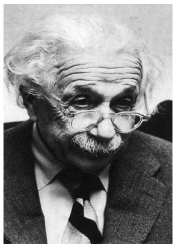
The internship was completed under the supervision of the Manager, Clinical Data Collection, Quality Resources and Decision Support Services. The project plan was presented to the Director of QRDSS for approval. The principle purpose of the work internship was to provide the Senior Management Team (SMT) of the IWK Health Centre with guidance and recommendations for implementing a policy for privacy impact assessments. The PIA tool would be used to evaluate the privacy, confidentiality and security of information systems that collect, store and use personal health information. The scope of the work included research and assessment of current standards of practice, privacy legislation, and the use of PIA's in Canada.

The project was assigned the following tasks.

- ✓ Research and assessment of the current standards of practice and the regulatory and compliance requirements for privacy assessments in Canada.
- ✓ Conduct an assessment of processes, resources and systems at the IWK to identify the human and monetary resources necessary to implement PIA's.
- ✓ Develop the necessary requirements to implement PIA's and other privacy tools to minimize the privacy and confidentiality risks.

This project was completed on a part-time basis over a period of 10 months in conjunction with other responsibilities in the Biomedical Engineering department. Although not in the original scope of this internship work was performed as a privacy and technology analyst supporting a Health Centre wide committee formed to evaluate new and emerging patient monitoring systems and networks. The position was responsible for assessing the privacy and confidentiality of health information collected by the systems being evaluated and assessed.

4. Relationship to Health Informatics



"Let every man judge according to his own standards, by what he has himself read, not by what others tell him."

Albert Einstein
1879-1955

"The field of Health Informatics deals with understanding the meaning and use of health information to support clinical care, health services administration, research and teaching. The program (Health Informatics) deals with the management and use of health information. As health informatics professionals it is important to understand the privacy landscape because health information can include personal information which is protected by privacy legislation. Canadians trust that the privacy and confidentiality of their personal health information will be protected. Privacy principles must therefore be embedded into the design of all systems which are collecting, storing and sharing of personal health information. This includes not only electronic information system but is also applicable to any paper based systems.

A Privacy Impact Assessment can be a valuable tool for Health Information Professionals. It can be used as a self-assessment toll to evaluate privacy and security elements in each project. It provides an assessment of compliance with applicable legislation and regulations pertaining to the protection of personal information. It assesses the technical safeguards for the protection of personal information and serves as a tool to examine policies and processes pertaining to the protection of personal information and to determine a projects compliance with the principles of the Canadian Standards Associations (CSA) Model Privacy Code for the protection of personal information (Appendix A).

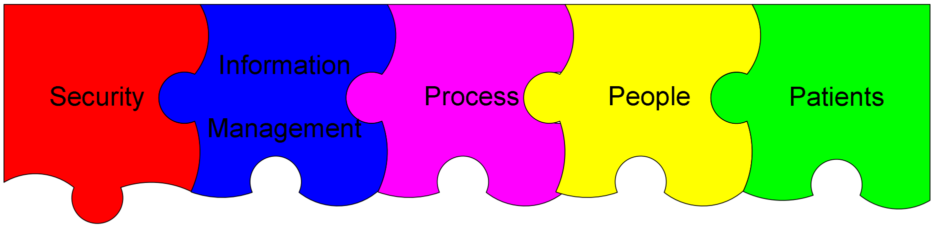


Figure 2 Privacy Practice Elements

As a minimum good privacy and confidentiality practice for health Information projects should include analysis of interconnectivity of the elements illustrated in Figure 2. All aspects of the patient and the relationship to the project should be considered. The people who will be accessing the system and any partners in the project must be identified. All system processes including the administration of the privacy and security aspects of the system should be evaluated. Security aspects including physical, technical, communications, database and operational safeguards used to protect personal information of the system must be considered. Knowledge of privacy framework and completing a PIA will assist in identifying gaps in these key elements.

4.1 Pan-Canada and Health Information Privacy and Confidentiality Framework

Recognizing the importance of privacy and confidentiality the Federal/Provincial/Territorial Conference of Deputy Ministers of Health tasked the Advisory Committee on Information and Emerging Technologies (ACIET) to develop a Pan-Canada and Health Information Privacy and Confidentiality Framework. The Pan-Canadian Health Information Privacy and Confidentiality Framework is a guide aimed at protecting the privacy and confidentiality of individuals with respect to their health information, while enabling the flow of information where appropriate to support effective health care, the management of the health system and an interoperable health record. It could also be used as a valuable tool to inform and influence privacy legislation within jurisdictions affecting personal health information. This Framework defines personal health information used as the basis for this internship report.

The definition of ***personal health information*** is information about an identifiable individual that relates to the:

- physical or mental health of the individual, or
- provision of health services to the individual, and may include:
  Information about the registration of the individual for the provision of health services.
- information about payments or eligibility for health care in respect to the individual,
- a number, symbol or particular assigned to an individual to uniquely identify the individual for health care purposes,
- any information about the individual that is collected in the course of the provision of health services to the individual, and
- information derived from the testing or examination of a body part or bodily substance.

4.2 Canada Infoway

Understanding and protecting privacy in the context of health informatics projects is also important given the fact that Canada Infoway is leading the development and implementation of *e*health projects. Canada Infoway is an independent, not-for-profit organization whose members are Canada's 14 federal, provincial and territorial Deputy Ministers of Health. The vision of Infoway is "A high-quality, sustainable and effective Canadian healthcare system supported by an infostructure that provides residents of Canada and their healthcare providers with timely, appropriate and secure access to the right information when and where they enter into the healthcare system. Respect for privacy is fundamental to this vision." The framework of privacy and security is fundamental to the blueprint shown in Figure 3.

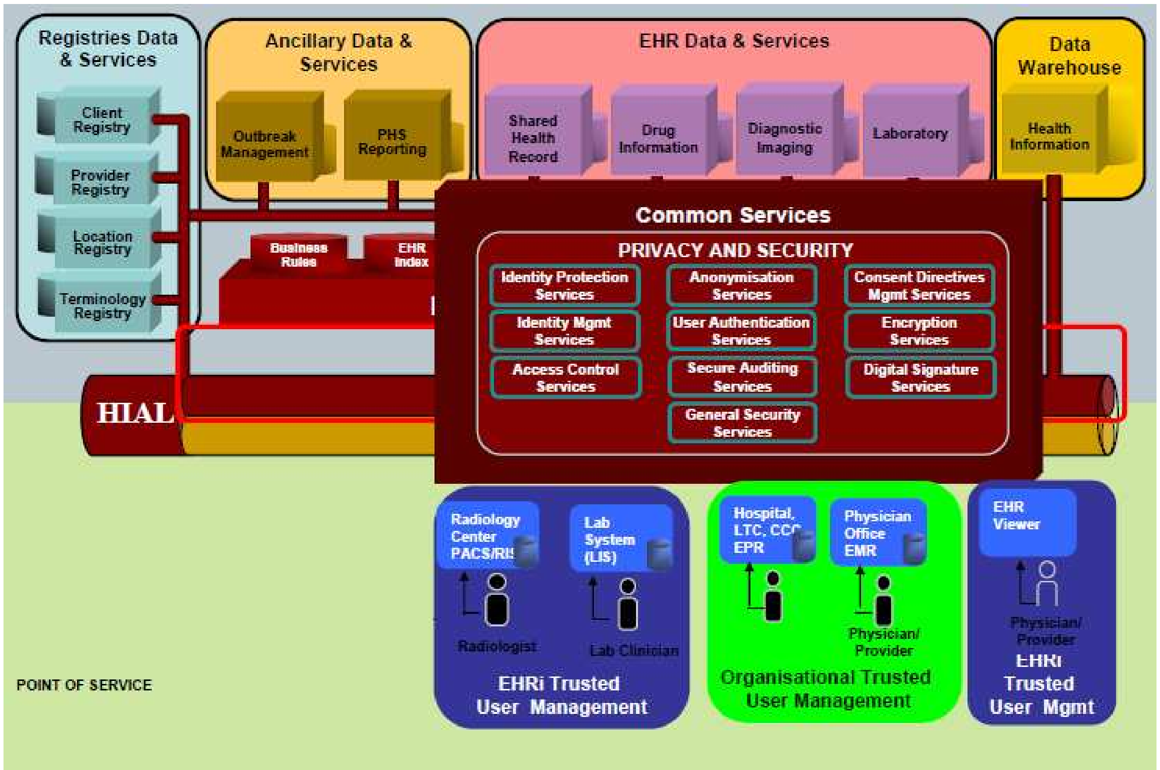


Figure 3 Canada Infoway Privacy and Confidentiality Blueprint

The Pan Canadian Privacy and security architecture is based on:
• Canadian CSA Privacy Model Code (Appendix A)
• Internationally recognized Information Security Management standards
• ACIET Pan Canadian Privacy and Confidentiality Framework

Key features of the blueprint for access to personal information includes

- Personal Health Information (PHI) is to be only accessed by authorized Healthcare providers. Provision for jurisdictional or regional access control rules applied in a consistent manner.

- Patients have the right to determine the purpose, when and

  who can access their PHI. Where applicable by law, PHI is only made available to a Healthcare provider if the appropriate jurisdictional and/or patient derived privacy rules are satisfied.

- Prevent unauthorized access to PHI. The use of encryption technologies to protect against unauthorized access (confidentiality and Integrity) to PHI whether in storage or during transmission.

- Ensure that Healthcare providers are uniquely identified, authenticated and authorized to access PHI in a trustworthy common manner notwithstanding where they access PHI Single sign on with one electronic credential (ID) recognized by all applications. Defining and applying standardized predefined roles across disparate healthcare applications. Creation and validation for Digital Signature on electronic documents, i.e. ePrescribing, proof of authoring of, and acceptance of reports Audit Trace required for consent override and access: a fundamental privacy requirement who, what, when, why has accessed PHI.

- Information not typically available can be accessed in emergency situations. Support for predefined conditions for overriding privacy and access control rules. Support for extensive audit traceability in cases of exception

- Concerns about the privacy risks of centralized data bases. Highly secure data centres. Federated data bases such that not all of a person’s data is within one database or in one data centre. Encrypt all PHI data. Privacy protective backup namely encrypted. Use mechanisms to allow for de-identification and re-identification of PHI. Centralized systems and databases have fewer points of system and user connection, thus fewer points of privacy and security risk.

4.3 Background to Privacy Impact Assessments

A PIA is a risk management tool used by decision makers to identify actual or potential effects that a proposed or existing information system, technology or program may have on individuals' privacy. It is important to note that the terms information system, technology, and program may also include the description of application, project, scheme, initiative or other endeavors that collect, store or disclose personal health information. A PIA should be conducted as early as possible in the decision process for the proposed design or change. It enables management to make informed decisions about information systems based on an understanding of the risks. It ensures that accountability for privacy issues in systems are incorporated in the design and development of information systems. It ensures a consistent format and structured process for analyzing both organizational and technical compliance with privacy principles. It ensures privacy protection is included in the modification and enhancement of information technology projects. It provides documentation on the flow of personal health information. All data flows from the point of data creation, to that of data destruction and all information-handling practices in between should be included in the PIA.

PIA's should be used in the identification and mitigation of risks arising from a new technology or the convergence of existing technologies. Examples of using a PIA would include use of electronic medical record (EMR) system or electronic health record (EHR) system, assessing the risks arising from a new program or from changing information handling practices with significant privacy effects, such as a proposal to use personal health information collected for treatment purposes. Another example would be the development of a research database or a proposal to integrate an EMR or EHR with a patient scheduling system.

A few key concerns about conducting PIA's include:

- ***A PIA adds expense to a project budget.***

  Although it may require adding resources and possibly a change in project timelines re-developing the project at a later date may be more costly.

- ***Conducting a PIA will introduce delays in the project.***

  The artifacts generated by the project may actually provide additional benefits of process diagrams, data flow tables and technical architecture diagrams which may benefit the implementation of the system. It also provides assurance that privacy risks have been identified and assessed.

- ***Identifying responsibility for maintaining the PIA***.

  Maintaining the investment in a PIA requires keeping the documentation correct and up to date. Continued development of the program or system will likely continue over time. If there are changes to a system or process the PIA will require updating to reflect changes. Responsibility for this maintenance process needs to be assigned.

Components of a Privacy Impact Assessment

Adapted from Management Board Office Province of Ontario

Conceptual Analysis	***Data Flow Analysis***	***Follow-up Analysis***
Prepare plain language description of scope and rational of proposed initiative	Analyze data flow using process diagrams. Through process	Review and analyze physical hardware and system design of proposed initiative to ensure compliance with privacy design requirements
Identify in a preliminary way potential privacy issues and risks, and key stakeholders	Assessment of proposals compliance with relevant privacy legislation, and general privacy principles	Provide final review of the proposed initiative
Provide a detailed description of essential aspects of the	Analyze risk based on privacy analysis of the initiative, and	Conduct a privacy and risk analysis of any new changes

proposal, including a policy analysis of major issues	identify possible solutions	to the proposed initiative
Document major flows of personal information.	Review design options, and identify outstanding privacy issues/concerns that have not been addressed	Conduct a privacy and risk analysis of any new changes to the proposed initiate relating to hardware and software design to insure compliance with relevant privacy legislation and general privacy principles
Compile environmental scan to review how other jurisdictions have handled a similar initiative	Prepare response for unresolved privacy issues	Prepare communications plan
Identify stakeholder issues and concerns		
Assessment of public reaction		

4.3 IWK Health Informatics Internship

Work completed for this Health Informatics Internship at the IWK consisted of:

- Development of a Privacy Impact Assessment Tool (PIAT).
- Privacy and technology analysis for patient monitoring and clinical information systems.

4.3.1 IWK Privacy Impact Assessment Tool

A privacy impact assessment tool was developed for the IWK as shown in Appendix B. The PIA tool will become part of the Privacy Policy at the IWK. The objective of the tool is to identify and mitigate privacy, confidentiality and security risks. The development of this tool was based on research conducted during a 10 month period. It focused on the issues of privacy, confidentiality and security of personal health information at the IWK. Conducting research for this internship was a challenging assignment. There is a “patchwork” of privacy laws in Canada with a federal government and thirteen provincial/territorial governments. Until recently much of the legislation has operated only in the public sector. Several provinces including Alberta, Saskatchewan, Manitoba and Ontario have enacted privacy statues aimed purposely at personal health information. In addition to research conducted on privacy laws and standards of practice there was also the opportunity to attend PIA workshops conducted by The Canadian Institute for Health Information (CIHI) and the Nova Scotia Department of Justice. Information was also gathered from interviews with various privacy professionals, health care corporations, and the Nova Scotia Department of Health Information, Access & Privacy Unit. The IWK PIA was developed based on the CSA Model Code for the Protection of Personal Information (Appendix A). This model is also known as the ten fair information practices and are defined in the following terms: accountability; identifying purpose; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

The IWK PIA is based on these fair information practices however it has been customized to the health and research sector. It includes the following elements:

- ✓ General Information – Includes project identification, key contacts and implementation dates.
- ✓ Project Description – Describes purpose, goals, objectives and flow chart of information collection and use.
- ✓ Collection, use and disclosure of personal information – Describes information to be collected, applicable regulations pertaining and the intended use of the information.
- ✓ Maintenance and Accuracy – Describes details of information retention and destruction methods.
- ✓ Safeguards, Security and Access – Describes storage, location, and access rights, audits, safeguards and controls for personal information.
- ✓ Mitigation of Risks – details to minimize or eliminate risks.
- ✓ Addition Information – Provision of any additional comments related to the PIA.

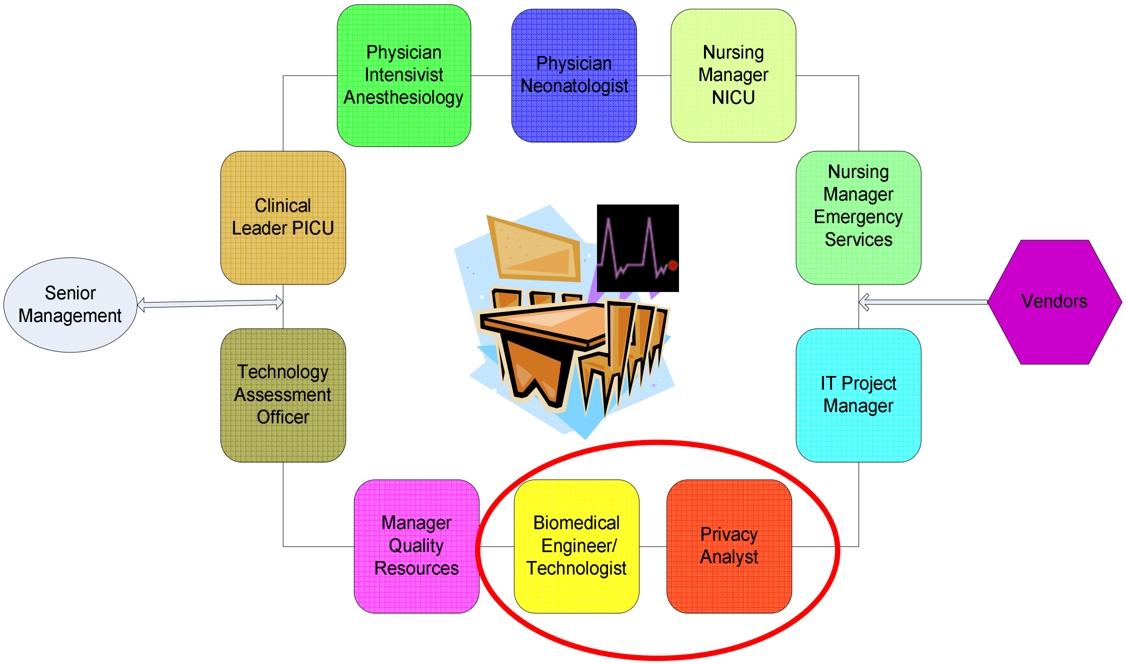
The final draft of the IWK PIA tool is currently in the process of receiving senior management approval as a policy for use at the health centre. It is expected to be trialed as a tool to assess privacy compliance of a new Poison Control database soon to be utilized. The PIA is expected to become an important part of the privacy policy for the IWK Health Centre. In the future all new projects/initiatives or those with a substantial change will be assessed using this tool.

4.3.2 Patient Monitoring Project

During the internship the author was requested to join the new patient monitoring committee established to assess and evaluate new patient monitoring systems. As an additional task to the PIA work underway the author was given responsible for the assessment of the privacy, confidentiality and security of patient information stored and accessed in the monitoring and data management systems under evaluation. The structure of this committee is shown in Figure 4. The red circle shows the areas responsibility for the author. A privacy survey was developed and completed based on interviews conducted with each of the invited vendors. The template developed and use is shown in Appendix C. Committee members consisted of clinical and technical specialist representing a broad range of expertise. It included physicians, nurses, healthcare managers, clinical leaders, IT project management, privacy specialist and biomedical engineering. The scope of this work was to evaluate the patient monitoring systems based on the specifications of the model shown in Figure 5. The system is designed as a solution for the monitoring and acquisition of patient physiological data and integration of the electronic medical record. In addition to monitoring and storing patient physiological data it provides an interface to other medical devices (ventilator, anesthesia etc.), hospital information systems (ADT), laboratory (LIS) and diagnostic imaging (PACS) systems. Areas of interest related to the study of health informatics include.

- Technology Assessment and Evaluation – Data acquisition, data use, information flow analysis and the evaluation of technology and data.
- Privacy Impact Assessment - Information flow, information storage and information access.
- Knowledge Management – Enterprise wide spectrum of disciplines and social networks.
- Communications and Reports – Used by committee for analysis
- Risk Analysis – Identifying and mitigation of Privacy Risks

IWK Health Centre
Patient Monitoring Committee 2005-2006



Physician Intensivist Anesthesiology
Physician Neonatologist
Nursing Manager NICU
Clinical Leader PICU
Nursing Manager Emergency Services
Senior Management
Vendors
Technology Assessment Officer
IT Project Manager
Manager Quality Resources
Biomedical Engineer/ Technologist
Privacy Analyst

Figure 4

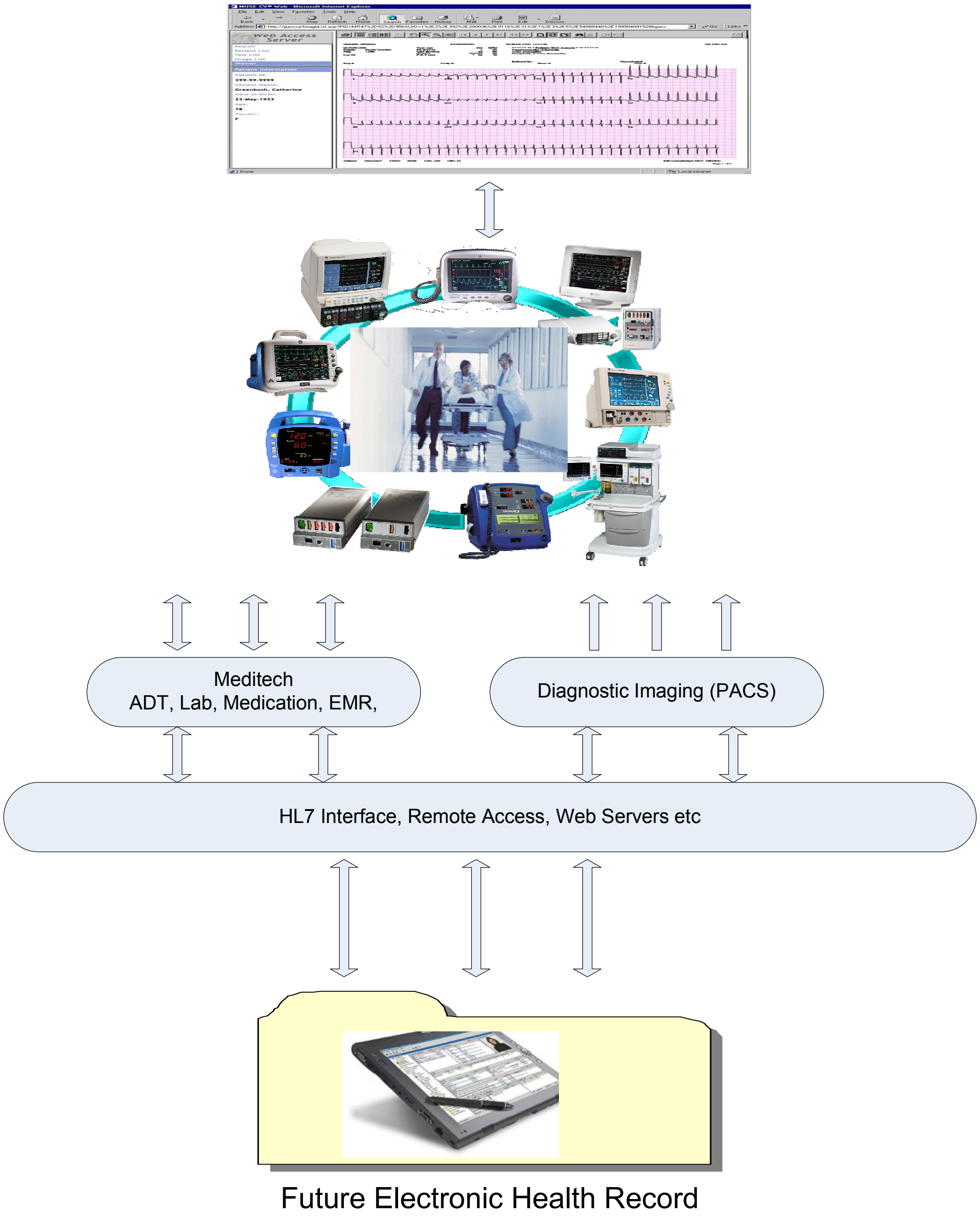

Meditech
ADT, Lab, Medication, EMR,
Diagnostic Imaging (PACS)
HL7 Interface, Remote Access, Web Servers etc
Future Electronic Health Record

Figure 5: System Requirements

4.4 Health Informatics Program Linkage

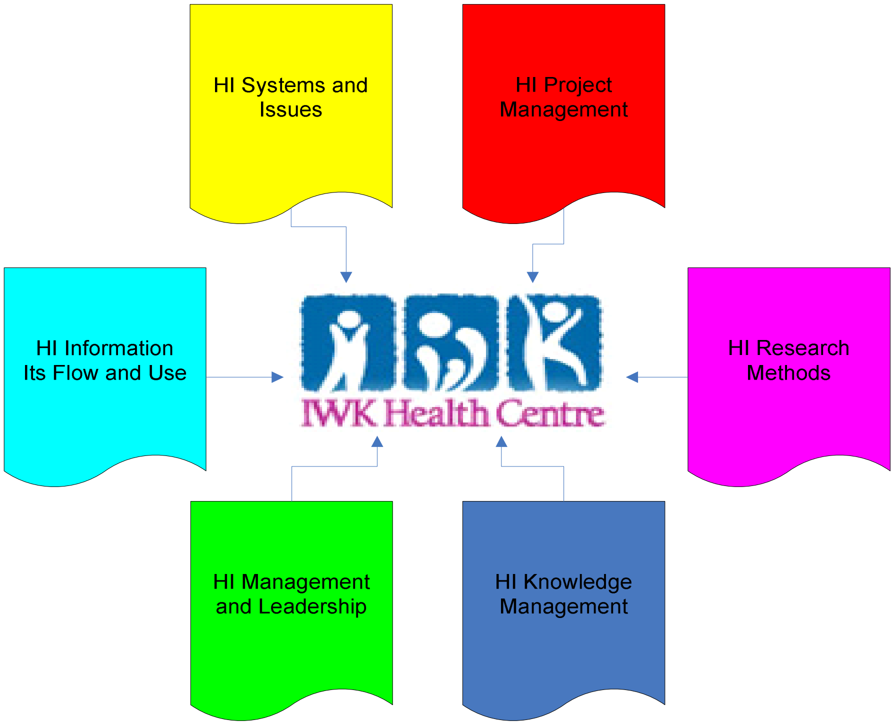


Figure 6 Health Informatics Program Linkages

The relationships shown in Figure 6 illustrate some of the linkages from the Dalhousie Health Informatics (HI) program completed that apply to the IWK Internship. The following are some of the highlights of components from health informatics courses completed to date which are applicable to this internship.

- ***HI Information Its Flow and Use*** – Developing data flow diagrams, and understanding HL7 interface issues. Flow diagrams are essential elements in developing PIA's and are used by both the reviewers and users. Understanding HL7 is a key component when discussing interfaces with patient monitoring systems and the IWK Meditech system.

- ***HI Systems and Issues*** – Understanding of clinical information systems and how they are used in a hospital environment. This course also provides background information relevant to the assessment and evaluation of technology. Information from this course was used in the assessment of patient monitoring systems.

- ***HI Management and Leadership*** – Understanding organizational behaviour and working in collaboration with the other stakeholders and participants of the patient monitoring as shown in Figure 4. Strong management skills were required to effectively develop questions and to implement solutions; especially when the users are often from varied disciplines and circumstances.

- ***HI Research Methods*** – Developing of a PIA for use in health care and understanding the kinds of information/technological support used and needed by researchers was useful in designing appropriate PIA questions.

- ***HI Knowledge Management (KM)*** **–** Knowledge management and knowledge transfer in health care organizations are key concepts in the success of any health information project. Understanding and applying knowledge elements was a key factor in the success of this internship. Working on a health care committee as large and diverse as the patient monitoring committee provided opportunities to understand social networks and collaborate with medical, administrative and technical staff on different levels. This collaboration is essential to the successful uptake of a project with an ownership cost in the $millions.

- ***HI Project Management*** **–** Project management skills are sought after in the healthcare environment. As with all successful projects the internship began with a plan, a scope, assigned tasks, deliverables and schedule to complete the tasks. These have proven to be valuable skills for health information projects such as this internship. The patient monitoring project provided a valuable opportunity to work in a project group with other health and IT professionals.

5. Problem Analysis - Privacy Legislation in Canada

"Currently, there is significant variation in privacy laws and data access policies across the country that poses a challenge for EHR systems that are dependent on inter-sectoral and inter-jurisdictional flows of personal health information. Differences in rules on how the scope of purpose is defined, the form of consent required, the conditions for substitute decision-making, the criteria for non-consensual access to personal health information, periods for retention of data and requirements for destruction, to name but a few, must be seriously addressed in order to enable the development of EHR system."

Kirby Report

Based on the Kirby Report and research conducted for this internship it is evident that PIA's for Health Information Systems may play a very important role in the future. The current vision of transferring patient information across provincial and territorial borders may be premature until there has been adequate discussion and consensus on privacy, confidentiality and security issues. The current patchwork of privacy laws in Canada consist of a mix of federal legislation and thirteen provincial/territorial legislations. Nova Scotia was the first province in Canada to enact a Freedom of Information Act in 1977. The original Act was replaced in 1994 by the Freedom of Information and Protection of Privacy Act (FOIPOP). Provinces and territories in all jurisdictions in the country have similar legislation. The enacted laws regulate the collection, use and disclosure of personal information in the public sector. During the 1990's laws specifically intended for health information emerged. Alberta, Manitoba, Saskatchewan and Ontario have all enacted such legislation. Quebec enacted health privacy legislation in the 1990's for the public sector. Some provinces such as Alberta (Health Information Act) require PIA's to be submitted to the Information and

Privacy Commissioner and must describe “how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information.” Review of the PIA by the Commissioner is required before the custodian implements any new system or practice. To date approximately 550 PIA’s in Alberta have been completed and submitted for approval. Appendix D shows the legislative requirements for a Privacy Impact Assessments Canada. Other provinces encourage the use of PIA’s. In Nova Scotia the province is expected in the near future to require PIA’s for all provincially funded projects. The provincial department of Justice is currently conducting PIA training sessions in preparation for this requirement.

The Romanow report also identifies the three main privacy issues that must be addressed for EHRs to become a reality in Canada in the next five to seven years are:

- The need for a more harmonized approach to privacy across all jurisdictions to allow for more consistent conditions for sharing personal health information among users and more consistent protection of personal health information for patients.
- The need to develop robust and effective privacy safeguards, policies and procedures that can be implemented in a pragmatic, practical and cost-effective manner.
- The need to build public confidence that personal health information will be protected in an electronic world.

Jurisdiction of Medical Services

The federal government in 2001 introduced the Personal Information Protection and Electronic Documentations Act (PIPEDA). It establishes the rules for personal information protection in the private sector. It is based on the CSA

Model Privacy Code (Appendix A). In 2004 it was extended to every organization that collects, uses or discloses personal information, including personal health information, in the course of commercial activity within a province, It will not apply where substantially similar provincial legislation is in effect.

The Governor in Council has issued exemption orders for organizations in the following provinces:

Ontario (November 28, 2005)
Alberta (October 12, 2004)
British Columbia (October 12, 2004)
Quebec (November 19 , 2003)

This legislation defines personal information as identifiable information about an individual. Personal health information is defined as:

(a) information concerning the physical or mental health of the individual;
(b) information concerning any health service provided to the individual;
(c) information concerning the donation by the individual or of any body part or of any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
(d) information that is collected in the course of providing health services to the individual; or
(e) information that is collected incidentally to the provision of health services to the individual.

Basically all the information found in a health record falls within this definition.

This has raised the very important question concerning whether the practice of medicine is a commercial activity. Industry Canada has ruled that a physician in private practice is engaged in commercial activity and falls under PIPEDA. However they have advised that hospitals are beyond the constitutional scope of the Act because the core of there activity is not commercial in nature. Where is the line drawn when we consider physicians working at hospitals?

As noted the provinces of Alberta, Saskatchewan, Manitoba and Ontario have privacy legislation which applies directly to health information. If the provinces can be declared similar to PIPEDA organizations within the province that collect, use and disclose health information in the course of commercial activities will have to comply with both the Health Information Act and PIPEDA rules. In some provincial health information statutes there are specific provisions aimed at security of EHRs.

Consent Requirements

Under PIPEDA knowledge and consent of the individual are required for the collection, use, or disclosure of personal information except where appropriate. If the use of the information is to be used for another purpose the organization must obtain individual consent for the new use. Under PIPDEA consent may be expressed or implied. Typically implied consent in the context of sharing personal health information is within the “circle of care”. This includes individuals and activities related to the care and treatment of the patient. The legal rules are challenging because the issue arises in that it may be nearly impossible to obtain truly informed consent from a patient regarding using and disclosing of information from health information systems. This is especially true when the future use of the information is not unforeseen. To require expressed consent for every use and disclosure of a patient’s information within a circle of care using an electronic means may bring the delivery of health care to a grind.

Another challenging issue is the secondary use of personal information for the purpose of research. Under PIPEDA secondary use of identifiable health information should be authorized by informed patient consent. The research landscape is evolving as knowledge and technological capacities continue to advance. The impact of new developments in research still needs to be determined. Particular to the concern for privacy protection is implementation of electronic health records across Canada over the next decade; discoveries in genomics and research on genetic-environmental interactions; increasing use of health-related databases, such as hospital and vital statistics records, for multiple purposes, including patient care and management, program management, public health functions and services (e.g. cancer screening, vaccinations, chronic disease risk factor surveillance, obesity interventions) and research.

6. Conclusions

Increasing public concern regarding privacy of personal information complicated by an array of non standardized privacy legislation in Canada creates a challenge for health informatics professionals. Proposed health information projects may carry increased risks for privacy violations of personal health information. It is therefore necessary to ensure privacy, confidentiality and security are designed into all projects which collect, use or disclose personal information. The field of Health Informatics deals with understanding the meaning and use of health information to support clinical care, health services administration, research and teaching. Developing a framework to formulate and answer questions related to these domains must have the premise of protecting personal health information. Developing a Privacy Impact Assessment is a valuable due diligence tool that will describe the system, document the flow of information, analyze threats and identify risks to privacy and document mitigation strategies.

7. Recommendations

Implementing PIA's into projects provides many benefits. The PIA artifacts provide the benefit of process diagrams, data flow tables and technical architecture diagrams which may support the implementation of the system. Although completing a PIA may require adding resources and possibly a change in project timelines re-developing the project at a later date may require greater resources. An important benefit not yet realized is the capturing of the process or information flow diagrams. These can be used to identify other potential linkages of information. It identifies *what* information is collected and *why* it is needed.

Opportunity now exist for moving forward and developing linkages with other systems *(where)* and *who* can benefit from the shared knowledge. This is a knowledge question that should be examined when developing and analyzing PIA's.

In a continued effort to develop a pan-Canadian electronic health record it may be wise to firstly consider implementation of a pan-Canadian health information privacy framework as a standard of reference to ensure compliance with jurisdictional privacy laws. However the privacy concerns are addressed it must not be aimed at satisfying the least significant privacy denominator but must be a robust interoperable system capable of safeguarding and protecting Canadians personal health information.

8. References

1. Health Canada. Pan-Canadian Health Information Privacy and Confidentiality Framework.
   Retrieved July 29, 2005 from
   http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index_e.html

2. Health Canada. Privacy Technology Review.
   Retrieved July 15, 2005 from
   http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2001-priv-tech/index_e.html

3. Health Canada. Commission's Final Report, *Building on Values: The Future of Health Care in Canada.* Final Report to Canadians November 28, 2002.
   Retrieved October 6, 2005 from
   http://www.hc-sc.gc.ca/english/care/romanow/index1.html ("Romanow Report")

4. Senate of Canada. The Standing Senate Committee on Social Affairs, Science and Technology, The Health of Canadians – The Federal Role Final Report, Volume Six: Recommendations for Reform. October 2002.
   Retrieved October 6, 2005 from
   http://www.parl.gc.ca/37/2/parlbus/commbus/senate/Com-e/soci-e/rep-e/repoct02vol6-e.htm ("Kirby Report")

5. Lypowy G. An Overview of the Privacy Impact Assessment and Its Applications Within Health Care in Canada. 2004, unpublished.

6. Treasury Board of Canada Secretariat. Privacy Impact Assessment Audit Guide. Retrieved July 08, 2005 from http://www.tbs-sct.gc.ca/ia-vi/policies-politiques/pia-efvp/pia-efvp_e.asp

7. Department of Justice Canada. Personal Information Protection and Electronic Documents Act 2000, c. 5
Retrieved July 08, 2005 from
http://laws.justice.gc.ca/en/P-8.6/258031.html

8. Clarke R. Privacy Impact Assessments (1999). Xamax Consultancy Pty Ltd, Canberra. Retrieved July 25, 2005 from
http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html

9. Ombudsman Manitoba. The Privacy Compliance Tool.
Retrieved July 25, 2005 from
http://www.ombudsman.mb.ca/compliance-phia.htm

10. Nova Scotia Department of Justice. Privacy Impact Assessment Training Workshop Manual. Received during Privacy Impact Assessment Training Workshop March 29, 2006.

11. University of Alberta, Health Law Institute, and University of Victoria, School of Health Information Science. Electronic Health Records and the Personal Information Protection and Electronic Documents Act.
Retrieved December 17, 2005 from
http://www.law.ualberta.ca/centres/hli/pdfs/ElectronicHealth.pdf

12. Ontario Hospital Association. 2003. Ontario eHealth Council. Guidleines for Managing Privacy, Data Protection and Security.

13. Canadian Standards Association. Model Code for the Protection of Personal Information
Retrieved July 22, 2005 from
http://www.csa.ca/standards/privacy/publications/Default.asp?language=english

14. Canadian Institute for Health Information. Conducting a Privacy Impact Assessment. Received during workshop December 3, 2004.

15. Canadian Institute for Health Information. Working Group 3: Privacy, Confidentiality, Data Integrity and Security, Background Document October 1997.

16. Privacy Impact Assessment, *A User's Guide.* Information and Privacy Office, Government of Ontario I & IT Strategy, Policy, Planning and Management Branch. June 2001.

17. Cornwall, A. Electronic Health Records: An International Perspective. Health Issues, 2002, Number 73, pp 19-23.

18. Vancouver Coastal Health, Privacy Impact Assessment
Retrieved August 11, 2005 from
http://www.vchri.ca/i/pdf/VCHPIAT.pdf

19. Newfoundland & Labrador Centre for Health Information, Privacy, Confidentiality and Access Principles and Guidelines for the Health Information Network. October 2004.
Retrieved August 26, 2005 from
http://www.nlchi.nf.ca/pdf/principles_guidelines_revised2004.pdf

20. Information and Privacy Commissioner/Ontario. Privacy and Boards of Directors: What You Don't Know Can Hurt You. November 2003.
Retrieved Sept 8, 2005 from
http://www.ipc.on.ca/docs/director.pdf

21. Information and Privacy Commissioner/Ontario. A Guide to the Personal Health Information Protection Act. December 2004.
Retrieved Sept 8, 2005 from
http://www.ipc.on.ca/docs/hguide-e.pdf

22. Information and Privacy Commissioner/Ontario. Putting the "E" into Privacy: Privacy Tips for Technology Leaders. August 17, 2000.
Retrieved Sept 8, 2005 from
http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=13119

Appendix A CSA's Privacy Code

1. Accountability
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent
The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

4. Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention
Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.

6. Accuracy
Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.

7. Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness
An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.

9. Individual Access
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

CSA Privacy Code

Appendix B

IWK Privacy Impact Assessment Tool

Privacy Impact Assessment (Preliminary Review)

A Privacy Impact Assessment (PIA) provides a framework to identify and mitigate the impact an activity may have on the privacy of an individual. It is used to determine whether a project, program, service, imitative, proposal, strategy, technology or information system (electronic and paper based) meet privacy requirements.

A PIA shall be required for activities that involve the collection, use or disclosure of personal information including:

- ✓ a new program or service
- ✓ a significant change to a program or service

This tool is based upon the Canadian Standards Association's "Model Code for the Protection of Personal Information which outlines internationally accepted "fair information practices that are the basis of privacy legislation and privacy policies across Canada.

The completion of a PIA for existing programs and services is also encouraged

For the purpose of this PIA "*personal information*" means any information recorded about an identifiable individual including but not limited to: name, address, age, gender, marital or family status, diagnosis, course of treatment, Social Insurance Number, Health Card Number, etc.

<u>Instructions</u>

Return completed PIA forms with all relevant documents to:

Privacy Officer
Quality Resources and Decision Support Services
IWK Health Centre

The Privacy Officer will review the completed PIA and provide further information and assistance as necessary.

1. General Information

a) Name of project/program:

b) Select project/program designation:

New project/program: □
Project/program with significant changes: □
Existing project/program: □

c) Provide contact information for the person responsible for answering questions regarding this project/program. Include name, department, location, telephone number and email.

Contact Person:
Department/Program area:
Location:
Telephone:
Email:

d) Provide key project/program dates. Include initiation date, implementation date(s), completion date, and other milestones, if applicable.

Initiation date: Implementation date: Completion date:	Explanation:

2. Description

a) Provide a brief explanation of the project, program, service or change.

b) Provide a description of the purpose, goals and objectives of the project/program. *What are you trying to accomplish with this project or program? Examples include improving delivery of patient care; education; research; statistics*

Purpose:

Goals:

Objectives:

c) Describe the need for collecting personal information
Why are you making this new project, program or change? Is it required by law, policy or standards?

d) Provide a description of the flow of personal information *(attach a flow chart if applicable)*

3. Collection, Use and Disclosure of Personal Information

a) Provide a list of all of the information that is to be collected and the intended use for the collection. (for example: name, address, telephone, number, diagnostic history)
example
Information to be collected: *Telephone number*
Intended use: *To update or follow up with clients*

Information to be Collected	Intended use of information

b) What is the source of the personal information? (e.g. patient, family member, third party provider, database, forms).

c) Are you aware of any laws, regulations, policies or guidelines regulating the collection, use and disclosure of the personal information in the project/program?

Yes □ No □ Don't know □
If Yes, describe or attach supporting documents

d) List all IWK Health Centre programs, external agencies and groups that will have access to the information. Explain why each requires access, the method of disclosure and what the information will be used for.

4. Consent

a) Has the individual consented to the collection, use and disclosure of personal information? Yes □ No □

If yes, describe the consent process. Attach any consent form(s)

If no, explain why consent was not required.

5. Maintenance and Accuracy

a) Describe how the personal information is kept accurate, complete and up-to-date for the requirements of the project/program

b) Provide details of the retention schedule or timetable for keeping the personal information collected? What is the plan and method for destruction of the information?

6. Safeguards, Security and Access

a) Will individuals have access to their own personal information? Yes □ No □

If yes describe the process for allowing access to their personal information and describe any limitations on access.

b) Where will the personal information be located? List all locations

How is personal information stored? Electronic format □ Paper format □

Is electronic information stored on servers? Yes □ No □
If yes specify location of servers:

Will users store information on individual’s computers or terminals? Yes □ No □

If there is a data repository, provide the name, description and geographical location of the repository.

c) List the users (positions, not names) who will have access to the personal information. Indicate a brief rationale for each user’s need to access the information and indicate if there are limitations or restrictions to this access.

d) Describe the administration safeguards in place to protect the personal information. e.g. have all users signed confidentially agreements.

e) Has all staff received training to familiarize them with the privacy, confidentiality and security policies and practices of the IWK Health Centre? Yes □ No □

f) Explain the process used to remove access to personal information when staff leave or change jobs or positions.

g) Describe the process in the case of a breach of privacy.

h) How is the personal information collected and transferred from the individual to the program/system? e.g. fax, email, paper, courier

i) Describe the techniques used to protect the security of the information?
e.g. locked file cabinets, encryption, passwords, and password change routine.

j) Is remote access to the information permitted? Yes □ No □

If yes, describe the method of access.

k) Is access to information monitored and audited? Yes □ No □

If yes describe:

l) Will the project/program be tested to ensure privacy controls are functioning? Yes □ No □

7. Mitigation of Privacy Risks

Provide any additional information, plans or proposals to minimize or eliminate risks to privacy of personal information in this project, program or change.

8. Additional Comments

Provide any additional comments or information related to the privacy impact assessment of this project, program or change.

Completed by: ___________________ Reviewed by: ____________________

Date: __________________________ Date: ___________________________

Appendix C *Sample of questions used for Vendor Interviews*

IWK Health Centre

Patient Monitoring Project Privacy Assessment Checklist

Vendor: ***Date:***

SAFEGUARDS

1. Does the application create, receive, store, maintain or transmit electronic Protected Health Information (ePHI)?
2. Is there a procedure for authorizing, establishing and modifying user access? How is access assigned?
3. Does the application facilitate automatic logoff capability?
4. Does the application have the capability of assigning unique identifiers to patients? Are personal or unique identifiers used to link or cross reference databases (ie Meditech)?
5. Describe what software, hardware, equipment, and physical components are in place to ensure secure data transmission, data storage, data security, and backup.
6. Does the system encrypt the data passing between the application and servers?
7. What is the retention schedule for patient information kept in the system? Is information archived?
8. Describe information flow from patient to information storage devices.
9. How is the personal information collected and transferred from the patient to the system/program? (ie example electronic, paper?)
10. Will the system be tested to ensure privacy controls are functioning?

AUDITING

11. Does the system maintain an audit log that records: username, user logon ID, date & time of logon, forms/screens accessed, user location, ID of patient/client records accessed, including remote access by vendor for support?
12. Does the audit log track/changes made during each user session?
13. Does the system prevent the deletion, overwriting, or modification of audit logs?
14. Does the information system maintain the audit logs for a prescribed time period and/or provide a mechanism for audit log archiving?

REMOTE ACCESS

15. Will the system be accessed remotely for service or audit purposes?
16. Is the information accessed remotely anonymized?
17. If information is accessed by Vendor? Describe the type of information accessed? If it is personal information what procedures are in place to ensure confidentiality?
18. Does vendor have confidentiality clauses protecting personal information accessed by representatives and third party providers? Do arrangements with external service providers contain confidentiality clauses?
19. Describe the procedures in place to address security violations by the Vendor. ***How will they respond to a breach of security?***
20. Will data be used for any other purposes? Research/ Statistics etc.

ADDITIONAL COMMENTS

Appendix D

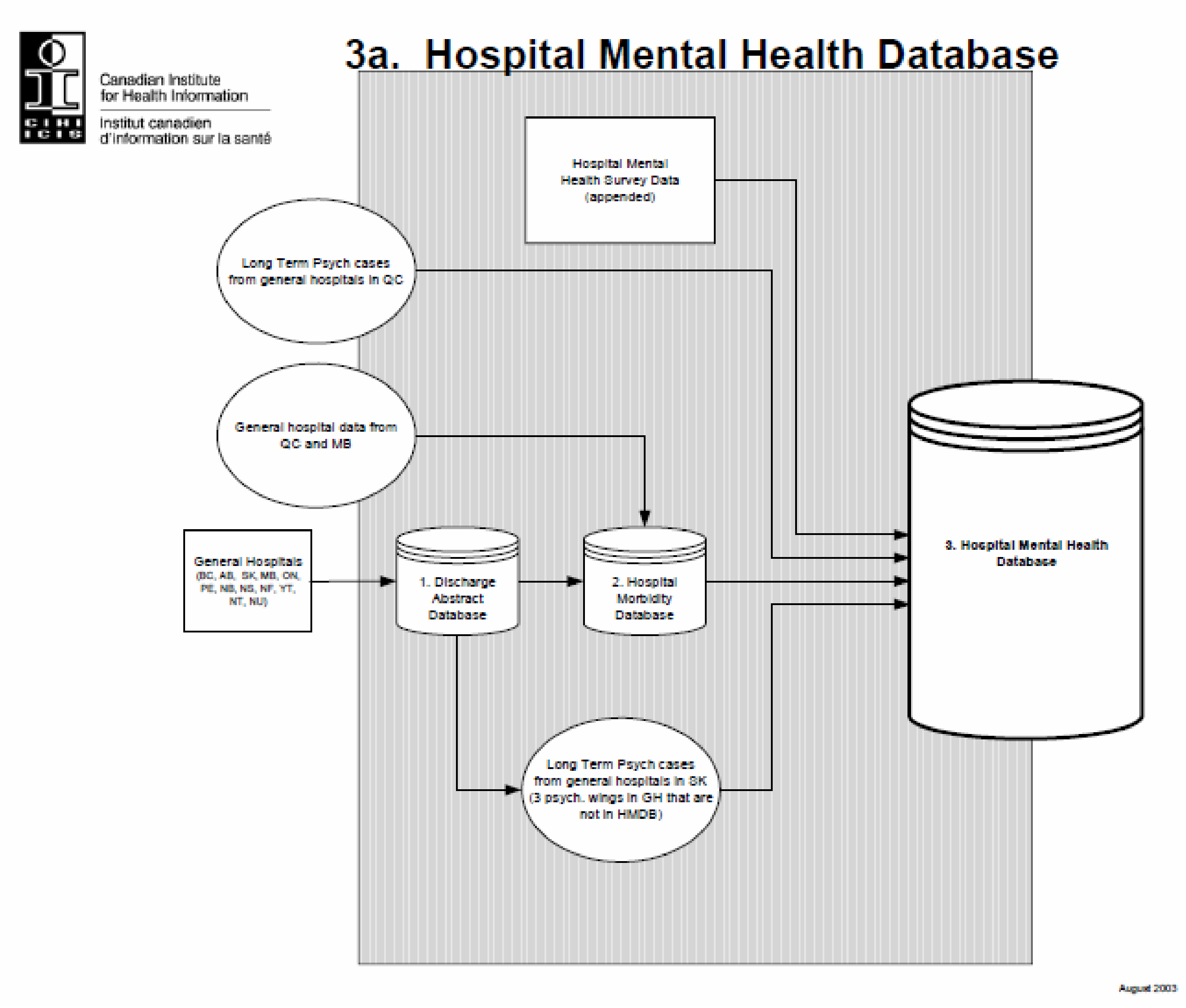
Legislative Requirements for a Privacy Impact Assessment

JURISDICTION	LEGISLATION	REQUIREMENTS SPECIFIED
Federal	*Personal Information Protection and Electronics Documents Act*	—
	Privacy Act	—
Nova Scotia	*Freedom of Information and Protection of Privacy Act*	—
Prince Edward Island	*Freedom of Information and Protection of Privacy Act*	—
New Brunswick	*Protection of Personal Information Act*	—
Newfoundland and Labrador	*Access to Information and Protection of Privacy Act*	—
Ontario	*Personal Health Information and Protection Act*	Section 6(3) subparagraph 5: A person who provides goods or services for the purpose of enabling a custodian to use electronic means to collect, use, modify, disclose, retain, or dispose of personal health information shall perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to, (i) threats, vulnerabilities and risks to the security and integrity of the personal health information, and (ii) how the services may affect the privacy of the individuals who are the subject of the information.
	Freedom of Information and Protection and Protection of Privacy Act, General Regulation	—
	Municipal Freedom of Information and Protection of Privacy Act	—
British Columbia	*Personal Information Protection Act*	—
	Freedom of Information and Protection of Privacy Act	Section 69(5): Public bodies which are ministries (i.e., excludes regional health authorities and hospitals) are required to conduct a privacy impact assessment for all new enactments, systems, projects or programs to determine whether the requirements of the Act are met. The privacy impact assessment must be conducted in accordance with the process/tool referenced in Schedule A attached hereto.
Alberta	*Health Information Act*	Sections 64, 70(2) and 71(2) and (3): Each custodian must prepare a privacy impact assessment and must submit it to the information and Privacy Commissioner for review and comment before implementing any proposed administrative practices and information systems or any proposed change to any such existing practices and systems in accordance with the privacy impact assessment tool referenced to Schedule A attached hereto. Section 46(5) Requirements for the Department to conduct a privacy impact assessment in certain situations)

Legislative Requirements for a Privacy Impact Assessment

JURISDICTION	LEGISLATION	REQUIREMENTS SPECIFIED
	Personal Information Protection Act	—
	Freedom of Information and Protection of Privacy Act	—
	Municipal Government Act	—
Saskatchewan	*The Health Information Protection Act*	—
	The Freedom of Information and Protection of Privacy Act	—
	The Local Authority Freedom of Information and Protection of Privacy Act	—
Manitoba	*Personal Health Information Act*	—
	The Freedom of Information and Protection of Privacy Act	
Quebec	*An act respecting the protection of personal information in the private sector*	—
	An act respecting access to documents held by public bodies and the protection of personal information	—
Yukon	*Access to Information and Protection of Privacy Act*	—
Northwest Territories	*Access to Information and Protection of Privacy Act*	—
Nunavut	*Access to Information and Protection of Privacy Act*	

Appendix E



Canadian Institute for Health Information
Institut canadien d'information sur la santé

3a. Hospital Mental Health Database

Hospital Mental Health Survey Data (appended)

Long Term Psych cases from general hospitals in QC

General hospital data from QC and MB

General Hospitals (BC, AB, SK, MB, ON, PE, NB, NS, NF, YT, NT, NU)

1. Discharge Abstract Database

2. Hospital Morbidity Database

Long Term Psych cases from general hospitals in SK (3 psych. wings in GH that are not in HMDB)

3. Hospital Mental Health Database

August 2003