Canada Health Infoway
Inforoute Santé du Canada

An overview of the

Electronic Health Record Privacy and Security

Conceptual Architecture

CONTENTS

1 Introduction 1

2 Infoway's Privacy and Security Project – an Overview 3

3 How Healthcare Professionals Access and Use Personal Health Information – Report #1 – Use case analysis 4

4 Defining the Privacy and Security Requirements - Report #2 5

5 The Privacy and Security Conceptual Architecture – Report #3 6

5.1 What is a conceptual architecture? 6

5.2 Why Privacy and Security Have Their Own Conceptual Architecture 6

6 The Privacy and Security Conceptual Architecture – Key Features 6

7 The Privacy and Security Architecture – How the Key Features Support Privacy Principles 7

7.1 CSA Principle 1 - Accountability: 7

7.2 CSA Principle 2 - Identifying Purposes 8

7.3 CSA Principle 3 - Consent 8

7.4 CSA Principle 4 - Limiting Collection 8

7.5 CSA Principles 5, 6, & 7 - Limiting use, disclosure and retention ; Accuracy ; Safeguards 8

7.6 CSA Principles 8, 9, &10 – Openness, Individual Access & Challenging Compliance 10

8 Other Special Features of the Architecture 10

9 Accessing the Interoperable EHR 12

10 Who Will Control the Interoperable EHR? - Governance 12

11 Getting There From Here: Interim States of the Architecture 13

12 Summary 13

1 Introduction

The electronic health record is needed to support the evolution of a modern healthcare system. This is recognized globally, and Canada is no exception.

To support Canada's Healthcare Renewal agenda, Canada Health Infoway was established by Health Canada in cooperation with the provinces. Its mandate is to accelerate the development and use of the electronic health record in an effort to improve Canadians' access to health services, enhance the quality of care and patient safety, and assist the healthcare system to become more efficient and effective.

The electronic health record as envisioned,

> "*… provides each individual in Canada with a secure and private lifetime record of their key health history and care within the health system. The record is available electronically to authorized health providers and the individual anywhere, anytime in support of high quality care. This record is designed to facilitate the sharing of data – across the continuum of care, across healthcare delivery organizations and across geographies."* [1]

The objective of the electronic health record is to get the right information to the right person at the right time. It is intended to give authorized health care providers rapid access to their patients' up-to-date health information, thereby enabling them to make better care decisions. In order to accomplish this, a network of interoperable electronic health record solutions – one that links clinics, hospitals, pharmacies and other points of care – is necessary.

The Need for the EHR

A recent study indicates EHRs for all Canadians could reduce healthcare costs by an estimated $4.7 to $7.3 billion annually.[2] Another report[3] estimated that implementation of comprehensive EHR systems across Canada would save taxpayers $39.8 billion over twenty years.

EHRs can already be shown to be increasing productivity and addressing health human resource shortages. One example is the Fraser Health Authority in British Columbia, where a system to access digital diagnostic imaging (x-rays) online improved radiologists' productivity by an estimated 20% and that of other specialists by 10%. Replicating such a system Canada-wide would effectively add the capacity of 260 radiologists and five to 10 million examinations. Shared diagnostic imaging systems would also save an estimated $350 million annually by reducing test duplication due to lost or misplaced results and by eliminating manual handling and storing of physical films.

The Need to Share and Protect Personal Health Information

Part of the challenge of creating an EHR lies in the great range and complexity of health-related information that will be held in the EHR. Another part of the challenge lies in the incompatibility of antiquated local systems. However, the fact that the EHR involves the sharing of personal health data from one part of the health system to another, for example from laboratories or diagnostic imaging clinics to the hospital or the doctor's office, presents an even more difficult challenge.

Health information is acknowledged to be the most sensitive of all personal information, even more sensitive than a person's financial information. The need to move healthcare information across the EHR system, while respecting patient privacy and rigorously protecting the confidentiality of the information, presents some of the biggest challenges to the development, adoption and acceptance of the EHR.

[1] Canada Health Infoway – Funding Agreement definition
[2] Canada Health Infoway's 10 Year Investment Strategy, page 10.
[3] Canada Health Infoway's 10 Year Investment Strategy, page 1.

Based on a study by EKOS in 2003 of 2300 Canadians, 86% of Canadians are moderately to extremely comfortable with the EHR, but they expect their personal health information to be properly protected and access to the information to be properly controlled. When asked what would make them more comfortable with the EHR, the top five responses were:

1. the ability to find out who accessed the record and when – 71%
2. make it a serious criminal offence for unauthorized access – 64%
3. a clear and accessible privacy policy – 61%
4. their ability to access, verify and correct record – 57%
5. that their doctor supported the EHR – 57%

This and other surveys suggest that the acceptance, use and benefits of EHR systems can only be realized if the systems are built to respect patient privacy by rigorously protecting the data from unauthorized access as well as auditing its use.

The intent of this paper is to provide healthcare executives and administrators, Information and Privacy Commissioners, and interested members of the public with an overview of Infoway's Privacy and Security Project and, in particular, to describe in brief, the Privacy and Security Architecture. Those involved in development of EHR solutions are advised to go directly to the source documents.

2 Infoway's Privacy and Security Project – an Overview

Beginning in the summer of 2004, Infoway spent a year tackling the complex privacy and computer security issues related to the interoperable electronic health record. The work produced three reports which lay the groundwork for building secure and privacy-protective EHR systems. All reports are available at http://knowledge.infoway-inforoute.ca/.

The first report presents an analysis of how healthcare professionals actually use healthcare information systems. The analysis considered the types of EHR system users who would potentially interact with the interoperable EHR, the various scenarios in which they would potentially use the EHR, and the potential uses of each component.

The second report sets out the privacy and security requirements for the handling of personal health information (PHI) within an interoperable EHR. It was released in February 2005 after being reviewed with representatives of governments from the majority of provinces and territories, as well as the federal government and national healthcare professional associations. The report provides a brief description and rationale for each requirement and addresses legislatively required and best practice privacy and security protections that are relevant to the interoperable EHR.

The third report builds on the first two reports and presents the privacy and security architecture. The architecture document was developed with input from an expert panel, in addition to a review by jurisdictional representatives and national healthcare provider associations during a series of validation workshops. The privacy and security conceptual architecture incorporating the feedback from stakeholders was published in the summer of 2005.

Finally, a privacy and security standards analysis was published in August of 2005 that considered the available standards for privacy and security and their potential applicability to the interoperable EHR.

3 How Healthcare Professionals Access and Use Personal Health Information – Report #1

In order to design a secure and privacy-protective EHR system, architects must understand how future users will interact with the system so they studied who would likely be using the system and how..

EHR future users are expected to include individuals such as:

- **family physicians who provide regular primary care to individual in clinics or private practice offices.**
- **physicians and emergency care providers who practice emergency medicine**.
- **medical specialists who provide care on a referral basis and who need access to basic information about the patient including** prescription drug profiles and laboratory test results.
- **nursing professionals** who provide front-line healthcare to patients in hospitals, clinics, community care settings and nursing homes.
- **pharmacists** who manage the filling of prescriptions and other administrative functions associated with dispensing prescription drugs. Pharmacists are also responsible for ensuring that patients receive the maximum benefit from prescription drugs and that they are not inadvertently given injurious drug combinations**.**
- **radiologists who view diagnostic images.** Significant investment has already been made in diagnostic imagining capabilities for the EHR such as x-rays, CT, MRI, and PET scans.
- **dental surgeons**, who would benefit from access to basic medical information on patients' allergies, drug sensitivities, etc.
- **paramedics** assisting in the delivery of emergency medical care.
- **laboratory technicians** who deal with laboratory examinations results.
- **public health officers** who are responsible for public health surveillance.
- **individual patients where access is permitted to portions or all of the PHI in the EHR.**

A range of scenarios were identified and then examined to determine the different ways the future users might interact with the EHR system during the encounter and how information about the patient would be recorded, accessed and updated. The scenarios were then deconstructed into separate components, for example, confirming the patient's identity, retrieving the patient's EHR, ordering a lab test, etc., and examined to see what aspects, if any, they shared. The use case analysis examined eight healthcare scenarios, two administrative scenarios, and forty-six separate components.

The analysis raised more than 20 issues relating to patient privacy and to the security of personal health information in the process of being transmitted, stored and delivered to healthcare professionals by EHR systems. Some issues were administrative (e.g., determining the members of a patient's healthcare team), others were technical (e.g., how to maintain confidentiality and informational integrity while data are in transit and storage) or procedural (e.g., how to ensure that the patient being treated matches the electronic record retrieved?). Various issues were related to patient choice (e.g., can a patient "opt out" of electronic health records?), and a few were related to the different patient consent models in the different provinces. The issues provided valuable information for the architects.

For the full report see "Electronic Health Record Privacy and Security Use Cases", available at http://knowledge.infoway-inforoute.ca/.

4 Defining the Privacy and Security Requirements - Report #2

Just as the system architects need to understand how the EHR system will be used, they also need to understand the legal and professional obligations related to privacy, confidentiality and security in order to determine if and how the system can support those obligations.

Obligations to protect personal health information are set out in an array of provincial, territorial and federal privacy laws in Canada. Many health care providers are also covered by professional codes of conduct. With input from over 100 individuals involved in privacy, security, law and health administration, over a period of six months, 114 privacy and security requirements were identified.

The requirements in summary are provided in Appendix A where they are mapped against two well known standards. The first is the Canadian Standards Association *Model Code for the Protection of Personal Informatio*n which is being used as the basis for much of the privacy legislation being developed in Canada and the second is the International Organization for Standardization (ISO) called ISO/IEC 17799 "*Code of Practice for Information Security Management.*which is already in active use in many Canadian healthcare organizations and jurisdictions.

As well as laying the foundation for the system's privacy and security architecture, the requirements form a highly useful resource for provincial ministries of health that are preparing tenders relating to building such systems. Several provincial ministries of health have indicated their intention to refer to and use the requirements to reduce the cost of the procurement process. Reference to a common set of requirements not only saves time and money in procurement, but it also helps vendors, who can then design systems that meet a uniform set of requirements in addition to supporting interoperability of systems.

The full description of the Privacy and Security Requirements is available at http://knowledge.infoway-inforoute.ca/.

5 The Privacy and Security Conceptual Architecture – Report #3

5.1 What is a conceptual architecture?

A conceptual architecture provides a high-level view of the component parts of the system and how those component parts will fit together. In 2003, Infoway published the *Electronic Health Record Solution Blueprint*. The *Blueprint* provides a comprehensive description of the components necessary for the interoperable EHR and describes, in broad terms, *how* the components are envisioned to work together. The *Blueprint* is essentially a conceptual architecture for the interoperable EHR.

"Conceptual" is not a euphemism for "vague". The conceptual architecture must provide enough detail to ensure the coherent planning of services across the interoperable EHR.

The conceptual architecture is also technology-neutral. In other words it does not mandate the use of any particular technology, product or vendor service, it simply describes how the system should work.

5.2 Why Privacy and Security Have Their Own Conceptual Architecture

The 2003 edition of the *Blueprint* did not fully articulate *how* privacy and security requirements would be met within the interoperable EHR. By constructing a conceptual architecture for privacy and security, developers are now provided with a coherent roadmap from which to design, build and deploy the products that will connect to, or form a part of, the interoperable EHR. The Privacy and Security Architecture will be incorporated into future versions of the *Blueprint.*

In addition, as noted earlier, privacy and security requirements are set out in many pieces of legislation across the country. By conducting the analysis and synthesizing the requirements into one generic PSCA document that can be adapted to meet the needs of individual jurisdiction's legislative framework, development costs can be reduced, the likelihood of adopting technologically based privacy enhancing practices is increased, as is the likelihood that similar solutions will be adopted, thereby supporting the principle of interoperability.

6 The Privacy and Security Conceptual Architecture – Key Features

Underlying the PSCA are the assumptions that:

- all personal health information requires the strictest level of confidence while it resides in, or is transmitted by, the EHR system
- all personal health information should be assigned a uniformly high priority status for the purposes of system availability

The PSCA sets out ten components, also referred to as 'services',that are critical to the privacy and security of personal health information in an interoperable electronic health record environment. These services include:

- User identity management services – activities related to accurately identifying users of the system, such as registering users, assigning roles that define access privileges, and managing changes in their status.
- User authentication services – those activities needed to establish the validity of the claimed identity of a user logging into the system.
- Access control services – models that can be used to control access to data based on either the individual's specific role in the health care system, their association with a group or discretionary access, whereby an individual, such as a physician, has authority to grant access to the record.
- Informational consent directives management services - activities related to recording, managing, applying, logging and overriding an individuals consent directives.

- Identity protection services - the real time de-identification and re-identification of personal information during storage and use of PHI.
- Anonymization services – activities related to removing all personal identifiers from a record to enable use of the data for secondary analysis and research purposes.
- Encryption services – activities related to creating, renewing and revoking encryption keys and the application of cryptography during the encryption of PHI within databases, in stored (archived) files, during PHI transmission and processes used during authentication of systems and system users.
- Digital signature services – activities related to the secure use of electronic signatures.
- Secure audit services – activities involved in secure logging of access to and use of the system.
- General security services – that address activities related to scanning for viruses, secure back-up, archiving data, destroying data, and restoration of data.

7 The Privacy and Security Architecture – How the Key Features Support Privacy Principles

The ten interrelated privacy principles set out in the Canadian Standards Association Model Code for the Protection of Personal Information are used as the basis for most privacy legislation in Canada.

Following is a description of how the key features directly or indirectly support the Principles set out in the CSA Model Code. The CSA principles in summary are followed by a description of the services in the PSCA that support the principle.

In this regard it is important to note that:

- the PSCA addresses those elements of the electronic health record that involve technology,
- technology can certainly support many aspects of privacy, but not all privacy requirements involve technology or have technological solutions.

7.1 CSA Principle 1 – Accountability for Personal Information:

The CSA Model Code states:

> “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. “

The CSA principle focuses primarily on identifying an individual(s) to be responsible for compliance with the privacy principles and for ensuring the organization has appropriate privacy policies and training in place. These are normally organizational functions.

The principle of accountability highlights the importance of governance to the effective functioning and acceptance of the EHR. by users and the public,. No matter how much care and attention is devoted to the technology behind the interoperable EHR, the effort will be undermined if the policies, procedures, practices, and training needed for proper and secure operation are neglected. Those involved in administering the system must know and understand the confidential nature of the data held in the EHR, and they must understand importance of following procedures necessary to ensure its secure operation. Effective governance of the interoperable EHR will require: clear articulation of accountability, setting of minimum standards, full elaboration of policies and procedures, and objective measurement of compliance. A full chapter of Report #3 is committed to the topic of governance and more work is underway on the topic.

7.2 CSA Principle 2 - Identifying Purposes for Personal Information

The CSA Model Code states:

> “ The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.”

The purposes for collection by any system must be identified by the organizations responsible for the specific collection. This requirement is articulated in the Privacy Requirements Report.

7.3 CSA Principle 3 – Information Consent

The CSA Model Code states:

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

The PSCA directly supports this principle through the *Consent Directives Management Service.* It allows individuals to grant, withhold or withdraw their consent for the collection, use or disclosure of their personal health information in accordance with applicable privacy legislation. The service makes it possible to take the privacy requirements related to consent, in tandem with an individual's specific consent directives, to control use and disclosure of information. This service allows patients to restrict access to specific components of their EHR or their complete EHR, consistent with the legislation in their jurisdiction. For example if permitted in legislation, a patient could restrict access to or disclosure of their prescription drug profile.

The Consent Directives Management Service enables this to be done automatically and in real time. It also allows for substitute decision makers to be identified (where applicable), and; it records the patient’s directives regarding which EHR system users are permitted to access his/her personal health information.

7.4 CSA Principle 4 - Limiting Collection

The CSA Model Code states:

> “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.”

The EHR is built in such a way as to make it very difficult to collect unnecessary personal information. The data to be collected must be determined during development of the specific system application. Decisions respecting what data is collected would be based on clinical needs and standards.

7.5 CSA Principles 5, 6, & 7 - Limiting use, disclosure and retention of Personal Information; Accuracy of Personal Information; Safeguards for Personal Information

The CSA Model Code states:

> “ Personal information shall not be used or disclosed for purposes other than those for which it was 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 fulfilment of those purposes.”
>
> “Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. “
>
> “Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. “

The principles are consistent with the following concepts to which security professionals often refer:

confidentiality – which means restricting access to information to a limited number of known and authorised individuals and keeping it secret from anyone else, The PSCA supports the premise that *all* personal health information requires the strictest level of confidence while it resides in or is transmitted by the EHR system, including:

1. repositories EHR data (such as patient medical profiles, lab tests, diagnostic images, etc.);
2. patient registry data (lists of patient names linked to health card numbers, etc.);
3. data in the registry of healthcare providers (listing healthcare professionals, the numbers of their licenses to practice, and other identifying information);
4. data in the user registry, including data obtained during registration;
5. security-critical data;
6. data transmitted to, from and within the system.

.

integrity - which means keeping the information from being changed by unauthorised systems or individuals , and

availability – which means ensuring the information is available when needed and that information systems stay up and running despite attempts by hackers to shut them down through interference, or despite natural or infrastructural disasters such as floods, blackouts, fires or earthquakes.

Following are features of the privacy and security architecture that directly or indirectly support the three privacy principles and organizational policies related to the principles.

The *Access Control Service* ensures that personal health information is available only to users with an identified need-to-know. Three types of access control are simultaneously supported:

1) role-based access control, where access to specific types of personal health information is based on the healthcare role of the user (e.g., a pharmacist);

2) work- group-based access control, which bases access privileges to a given patient's record on the user's membership in one or more relevant work groups (such as a clinical teams in a hospital or physicians working in a family practice group); and

3) discretionary access control, which allows users with a legitimate access to a patient's EHR (e.g., a family physician) to grant access to newly legitimated users who have no previously established relationship to that patient's EHR (e.g., a specialist to whom the patient is being referred).

The ‘right information’ for certain authorized research purposes may involve making non-identifiable health information available to a researcher. The *Anonymisation Service* takes the relevant personal health information representing an identifiable individual and then removes all personal identifiers, such as the patient’s name, address or birthplace. The Service can also, if required, apply a unique or meaningless identifier to the record (pseudonymisation). The goal is to make information accessible to healthcare researchers and administrators without infringing on patient privacy.

The *Encryption Service* maintains the confidentiality and integrity of personal health information by using cryptography to render the data unintelligible while they are stored within databases, in backup files and while being electronically transmitted to and from physician offices, hospitals and other healthcare organisations.

A *Secure Audit Service* records privacy and security-related events in an event log, including any emergency access via the EHR system to any patient's record. It also provides for the implementation of privacy protective log files which may contain PHI or other sensitive data.

7.6 CSA Principles 8, 9, &10 – Openness about Personal Information, Individual Access to Personal Information & Challenging Compliance

The CSA Model Code states:

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

The above are governance matters that need to be addressed in an organization’s policies, principles and contracts. At the same time, several of the PSCA services combined, support the ability of the organization to provide the individual with a detailed record of what information is in the EHR, who has accessed it, and when and what transactions occurred with the information over time.

8 Other Protective Features of the Architecture

Security Layering

Anyone who has ever used computers knows how effective they can be at revealing the fallibility of human ingenuity. What if the cryptography described in the *Encryption Service* above is not implemented properly? What if someone fraudulently becomes a registered user, despite the protections built into the *User Identity Management Service?* What if the User A*uthentication Service* is cleverly circumvented by a hacker? What if the *Access Control Service* allows a physician to access a record to which she shouldn't have access?

The privacy and security architecture has been designed with human fallibility in mind. The ten privacy and security services are layered together to stand as multiple barriers between an unauthorised access-to-information and a patient's personal health information. Like a treasure hunter trying to open a nested series of cleverly locked Russian dolls containing a tiny treasure in the innermost one, an unauthorised third party needs to break through many consecutive barriers before gaining access to confidential information stored inside the interoperable EHR. Most importantly, those barriers do not depend upon each other to maintain their integrity. Breach one and the others stand. This is what information security experts call *defence-in-depth*. It is the cornerstone of designing robust and highly secure systems.

The *Access Control Service* and the *Audit Service* are examples of this layering of privacy and security services. Even if a physician obtained access to a record that he or she had no need to access, the *Audit Service* would log the access. The *Audit Service* also contains analytic tools that can look for unusual patterns of access and report them to a privacy officer. The *Audit Service* is independent of the *Access Control Service* and does not depend on it to function properly (the *Access Control Service* is equally independent). Separately, each provides powerful protection against, and detection of unauthorised access. Together, they provide even more robust protection.

Another example of layering is the combination of the *Authentication Service* and the *Encryption Service*. The *Authentication Service* prevents access to the system by unauthorised third parties. However, if a hacker were to somehow circumvent the system and directly access the underlying databases of information, or a backup tape misplaced the data held within the system or backup media can be encrypted and therefore useless to the interloper.

Protecting Patient Identities

Let's consider the question posed above, "what if the cryptography in the *Encryption Service* is not implemented properly?" Cryptography is not the only proposed way to protect the identities of patients.

An *Identity Protection Service* will facilitate the storage of personal information that uniquely identifies individuals (e.g. name, address, health card number, etc.) in a repository that remains separate from health information relating to the patient's care and treatment, diagnosis, etc. One database contains identifying information (e.g. name, address, emergency contact information) and is indexed by an individual's identifiers (such as a health card or health insurance number). A separate database contains health information stored under an individual's EHR client identifier (ECID), a meaningless but unique number that is only known or used internally within the interoperable EHR's implementation in a given jurisdiction. A cross-reference table maps an individual's public identifiers to his/her corresponding ECID. Without access to the cross-reference table, no one, not even a system administrator, can figure out which health record belongs to whom, and only the *Identity Protection Service* can access the cross-reference table. Without accessing the data through this service, individuals cannot be linked to their healthcare information. The whole series of defences used, then, makes unauthorised access to any comprehensible form of personal health information very difficult. Decrypting a database of lab test results, for example, may tell you that some of the patients have tested positive for HIV but not who they are, since you are unable to access the *Identity Protection Service* to look up their ECIDs. The *Identity Protection Service* can only be accessed through the *Access Control Service* which in turn can only be accessed through the *Authentication Service*.

The *Identity Protection Service* also makes it possible to provide health information to authorised researchers and public health surveillance officials without revealing patient identities. The *Identity Protection Service* can identify each patient by a pseudonym (which could be a meaningless number) and can further ensure that each pseudonym is never linked to a patient's unique personal identifiers, such as their health card number, name or address. Different pseudonyms can be also be generated for each research project, thereby reducing the likelihood that researchers obtaining many sets of data could match attributes to create an identifiable record. Pseudonyms could also be deleted after the project ends, so that only specific data elements germane to the research are maintained. In this way, the risk of revealing the identity of an individual is greatly diminished yet the value of the data for research is maintained.

The ability to track a record over time is critical to much of the outcomes analyses currently being undertaken to evaluate treatments. By using pseudonyms, all the records for "patient X" can still be accumulated over a period of years without ever revealing the identity of "patient X".

Where Sensitive Data will be Stored

The PSCA envisions multiple data repositories that contain subsets of the health information contained in hospital records and in physician offices and clinics. Single, massive repositories create risks not only from a privacy perspective but also from a system design perspective (*a single point of failure.*) Instead, most provincial jurisdictions will likely operate their own EHR data repositories. In large provinces, they may be split into smaller regional repositories. Alternatively, the smaller provinces and territories may jointly administer regional repositories that span provincial or territorial boundaries.

Patient Control Over Selected Data

As noted earlier, the architecture also allows for patients to restrict access to certain portions of their health information and to give instructions to a healthcare professional, such as a family physician, about the circumstances (if any) under which the information can be shared with another healthcare professional. The architecture accommodates two options.

1. Leaving the restricted information in its original location (for example, within a physician's office) and storing a notation in the repository that further information can be obtained from the physician in the event of a medical emergency. In this case the specified information never leaves the doctor's office. However, as a consequence the information may not be available when needed during a medical emergency, since the patient's doctor may not be reachable on the telephone or online.

2. Encrypting a copy of the restricted information and storing it in the repository along with a copy of the associated consent directive(s) and programming the Consent *Directives Management Service* to make this information available to authorised emergency healthcare professionals when needed and to audit access to the information. This approach has the advantage that the information will always be available in the event of a medical emergency. It has the disadvantage that the very information most worrying to the patient still ends up in a regional repository, however well protected it might be.

9 Accessing the Interoperable EHR

Users of the interoperable EHR will connect to the system in one of two distinctly different ways. Healthcare organisations, such as hospitals, have information systems that are capable of direct connection to the interoperable EHR. Authorised members of these organisations will gain access to EHR data through such interconnected information systems. But there are many healthcare professionals, including many thousands of physicians in small family practices, who are not affiliated with a large healthcare organisation and thus do not have access to such interconnected information systems. They need to be able to access the interoperable EHR via their computer's web browser. Both sets of users pose very different challenges to the secure and privacy-protective management of the interoperable EHR and both are addressed by the PSCA.

The first situation will take advantage of the security systems already in place in healthcare organizations such as a unique user ID, authentication processes (password or more sophisticated means such as biometrics), and security role assignments (physician, admissions clerk, etc.) At the same time, considerable care must be taken to make sure that the security of the interoperable EHR is not compromised by legacy systems that may be less robust than newer systems. As such, the PSCA requires standards by which to measure the performance of such systems and assess their trustworthiness. The organisation must fulfill these requirements for trusted connections before their users can access the interoperable EHR via the organisation's information management system.

Healthcare professionals who are not affiliated with a large healthcare organisation and who do not have access to institutional information systems will need a different route to the interoperable EHR. So too will institutional users who also want to obtain access while away from the organisation's IT system (e.g., while visiting a nursing home). This way of connecting users to the interoperable EHR involves a very different set of challenges than those encountered in connecting users via a healthcare organisation's information system. Each user must be registered and their authority profile determined. Then the system must be able to authenticate the users before they are allowed to access the interoperable EHR. Most importantly, there is the challenge of ensuring that privacy and security are never compromised as information flows from the interoperable EHR to the health professional's web browser.

With two distinct ways of connecting to the interoperable EHR, it is critically important that one route be no less secure or privacy-protective than the other. It is a fundamental design feature of the architecture that there be no back-door access to personal health information. Whichever route users take to accessing the interoperable EHR, the architecture will ensure that the privacy and security requirements discussed in section 4 are met.

10 Who Will Control the Interoperable EHR? - Governance

Governance issues surfaced during the PSCA consultative process. Decisions relating to matters such as the rules that govern the secure daily operations of an EHR, the transfer of personal health information across interoperable systems; the rules for data exchange from one province to another, and protocols for handling complaints or disputes require attention and policy resolution. Further work is underway to support discussion on these matter as it is recognized that the success of the interoperable EHR depends in part on governance issues being adequately addressed.

11 Getting There From Here: Interim States of the Architecture

The interoperable EHR will not be built in a day. When it is built, not every clinic or hospital system in Canada will immediately connect to it. It is essential, therefore, that plans allow for the implementation of the interoperable EHR to evolve over a period of years. For the purposes of this document, therefore, a distinction is drawn between the desired future state of privacy and security in the interoperable EHR (i.e., the long-term vision of how these services will operate), and interim states that allow existing POS systems to be connected with only modest changes to existing systems and workflows.

The privacy and security services discussed so far describe a desired future state in which the privacy and security conceptual architecture has been fully deployed. Infoway is currently working with provincial and territorial ministries of health to help them implement the privacy and security conceptual architecture as part of their projects.

12 Summary

Designing and implementing EHRs will be an expensive and complex undertaking over time. Implementation has to integrate information technology, privacy and security services, and governance issues. None can be neglected, or underfunded without putting in jeopardy the entire enterprise.

Respecting privacy and maintaining confidentiality of personal health information is fundamental to the EHR. The PSCA was developed to provide system developers with guidance on the features that need to be considered when developing a privacy sensitive and secure interoperable EHR system that complies with requirements set out in legislation and professional codes of conduct.

The PSCA presents a suite of services that may not be necessary for every application. They can be customized to meet the needs of the application and the privacy requirements of each jurisdiction.

The PSCA presents approaches that support the use of technology to support privacy principles.

The PSCA represents current thinking. As systems are developed, and other needs of the health system and privacy requirements are more clearly articulated, the PSCA will evolve.

For more detail or description of the Architecture and the services the reader is directed to the following source reports available at http://knowledge.infoway-inforoute.ca/:

Canada Health Infoway, *EHRS Blueprint: An Interoperable EHR Framework*, July 2003

Canada Health Infoway, *Electronic Health Record Privacy and Security Use Cases,* 2004

Canada Health Infoway, *Electronic Health Record Privacy and Security Requirements,* 2005

Canada Health Infoway, *Electronic Health Record Privacy and Security Standards Review,* 2005

Booz-Allen-Hamilton, *Canada Health Infoway's 10 Year Investment Strategy*, 2005

APPENDIX A – 1

Privacy and/or Security Requirements mapped to CSA Model Code Principles

As will become evident not all of the EHR privacy requirements are technical. Some are policy-related and many others relate to system administration. Interested readers can find a full discussion of all the privacy requirements in section 4 of *Canada Health Infoway, Electronic Health Record Privacy and Security Requirements,* version 1.1, June 2005, available at http://knowledge.infoway-inforoute.ca/.

Following are Privacy and Security Requirements mapped to the relevant CSA Model Code Principle. Privacy requirements are designated by the abbreviation PR and Security requirements by the abbreviation SR.

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. "

PR 1 Accountable person

Organisations that share or host components that store PHI must designate and publicly name an individual who is accountable for facilitating compliance with applicable data protection legislation and the following privacy requirements.

PR 2 Third Party Agreements

Organisations that share or host components that store PHI must use contractual means to provide a comparable level of privacy protection while a third party, such as a service provider, is processing PHI.

PR 3 Privacy Policy

Organisations that share or host components that store PHI must implement policies and practices that Implement procedures to protect PHI, establish procedures to receive and respond to privacy related complaints and inquiries, train and communicate to users information about the organisation's privacy policies and practices.

PR 4 Privacy Impact Assessments

Organisations that share or host components that store PHI, should assess, by means of a Privacy Impact Assessment, the risks to personal privacy associated with implementation of the hosted components and should implement appropriate privacy controls to mitigate identified risks.

SR 1 Threat Risk Assessment

Organisations that share or host components that store PHI must should – assess Information Technology threats and risks (TRA). The TRA process should also inform the PIA process in regard to privacy risks associated with the use of specific technologies.

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."

PR 5 Identifying Purposes for Collection, Use and Disclosure
Organisations that share or host components that store PHI must a) identify all the purposes for which PHI will be collected, used, and disclosed at or before the time it is collected; and b)

make a reasonable effort to inform patient/persons of these purposes, in a readily understandable manner, prior to collecting their personal health information.

PR 7 Limitation of Collection to Identified Purposes

*Organisations that share or host components that store PHI should only collect PHI necessary to fulfill the purposes that they have identified.**Error! Reference source not found.**).*

3. **Consent**:

The CSA Model Code states:

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

Laws may require different types of patient consent for specific collections, uses and disclosures of personal health information. An organisation should be able to demonstrate that it complied with applicable legislative requirements and that the patient had a reasonable opportunity to know that information was going to be collected and used for specific purposes. Patient consent is a complex and multifaceted subject and as a result, nine of the EHR privacy requirements deal with consent. These requirements are;

PR 8 Obtaining Knowledgeable Consent

Except where inappropriate (e.g. specifically exempted by law or professional code of practice), Organisations that share or host components that store PHI should obtain the knowledge and consent of each patient/person for the collection, use or disclosure of his or her PHI —and where required by law, must— obtain the knowledge and consent of each patient/person for the collection, use or disclosure of his or her PHI.

PR 9 Recording Consent in POS Systems

Organisations that share or host components that store PHI where required by law, must be able to record a patient/person's consent directives, including the withholding, withdrawal or revocation of consent.

PR 10 Associating Consent with PHI in POS Systems

Organisations that share or host components that store PHI record a patient/person's consent directives, including the withholding, withdrawal or revocation of consent, such systems must transmit these consent directives to the interoperable EHR, in a consistent form, whenever they transmit the associated PHI.

PR 11 Recording Consent in the interoperable EHR

Organisations that share or host components that store PHI where required by law, must be able to record a patient/person's consent directives, including the withholding, withdrawal or revocation of consent and must be able to do so in a way that allows each jurisdiction to comply with its own legal requirements on consent.

PR 12 Associating Consent Directives with PHI in the EHRi

When consent is required by law, whenever receiving, storing, processing, or transmitting PHI, the EHRi must be able to: a) maintain the association between this data and the consent directives under which it may be used or disclosed; b) process these consent directives before transmitting the associated data and block the transmission where it would violate the directives and c) notify the requestor whenever data is blocked.

PR 13 Logging the Application of Consent Directives

Organisations that share or host components that store PHI must be able to: a) log when the processing of consent directives item b) prohibits the transmission of data and log the identity of any user who overrides a patient/person's consent directives, the reason for the consent override, and the date and time when the consent override occurred and alert the individual accountable for facilitating privacy compliance in the organisation.

PR 14 Implications of Consent Directives

Organisations that share or host components that store PHI should ensure patients/persons are informed about the potential implications of their consent directives, including directives for locking or masking PHI.

PR 15 Recording Identities of Substitute Decision Makers

Where required to do so by law ,the organisations that share or host components that store PHI must have the ability to indicate when consent is given on behalf of a patient/person by a substitute decision maker (e.g. consent given by an authorized representative), as well as identify this substitute decision maker and the substitute decision maker's relation to the patient/person.

PR 16 No Coerced Consent

Organisations that share or host components that store PHI must not, as a condition of the supply of a service, require a patient/person to consent to the collection, use or disclosure of PHI beyond that required to fulfill the explicitly specified and legitimate purposes.

4. **Limiting collection**

The CSA Model Code states:

> "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."

Personal health information should not be collected indiscriminately and the interoperable EHR must ensure that collection of personal health information is limited to that which is necessary for the provision of care. This is stated in a single requirement for limiting collection of personal health information:

PR 17 Collecting Information by Fair and Lawful Means

Organisations that share or host components that store PHI must not collect PHI by misleading or deceiving patients/persons or healthcare providers about the purposes for which information is being collected.

5. **Limiting use, disclosure and retention of personal health information:**

The CSA Model Code states:

> " Personal information shall not be used or disclosed for purposes other than those for which it was 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 fulfilment of those purposes."

After organisations have identified the purposes for which they collect personal health information and have sought appropriate patient consent for these purposes, it is imperative that they then only use, disclose and retain that information for these purposes and no others. Four EHR requirements relate to this privacy principle.

PR 18 Limiting Use and Disclosure of Personal Health Information to Identified Purposes

Organisations that share or host components that store PHI must only use or disclose PHI for purposes consistent with those for which it was collected, except with the consent of the patient/person or as permitted or required by law

PR 19 Logging Access, Modification, and Disclosure

Organisations that share or host components that store PHI must a) have a mechanism to record every access, modification or disclosure of PHI, together with the time and identity of the accessing user and where required by law, have mechanisms to alert the organisation's individual accountable for privacy when it is suspected that PHI has been accessed, used or disclosed inappropriately.

PR 20 Notifying Patients/Persons of Inappropriate Access, Use or Disclosure

Organisations that share or host components that store PHI should notify patients/persons when it is determined that his or her PHI has been inappropriately accessed, used or disclosed in accordance with applicable laws, regulations and organisational policies and procedures.

PR 21 Retaining Records

Organisations that share or host components that store PHI must retain PHI in accordance with record-keeping requirements outlined in legislation; and should develop guidelines and implement procedures with respect to the retention of PHI, including minimum and maximum retention periods.

6. **Accuracy**

The CSA Model Code states:

> "Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. "

Personal health information must be sufficiently accurate, complete and up-to-date to be of use in patient diagnosis and treatment. One of the 29 EHR privacy requirements deals with accuracy.

PR 22 Accuracy

Organisations that share or host components that store PHI must take reasonable steps or make a reasonable effort to: a) ensure that PHI is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used, including disclosures of PHI to third parties; and b) accurately identify a patient/person when accessing or modifying his or her PHI

PR 22a Denoting Patients/Persons At Elevated Risk

Organisations that share or host components that store PHI must provide functions for marking records of selected patients/persons and subsequently making accesses to such data subject to mandatory auditing by the individual accountable for privacy compliance in the organisation.

7. **Safeguards**

The CSA Model Code states:

> "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. "

Appropriate security safeguards must protect personal health information against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification. While only two EHR privacy requirements relate to safeguards, the specification of these safeguards has led to the specification of many security requirements. The security requirements, at the end of this list, are further mapped against the ISO standards.

PR 22b Training Users and Raising Privacy Awareness

Organisations that share or host components that store PHI must ensure that privacy education and training and regular updates in organisational privacy policies and procedures are provided to each permanent or temporary employee or third-party contractor who is a registered user of a POS connected to the EHRi or who has access to hosted components of the EHRi.

SR 65 Authenticating EHRi Network Access

Organisations that share or host components that store PHI must ensure that all connections to remote servers and applications are authenticated. This includes connections via the Internet.

SR 37 Protecting Storage of Unencrypted PHI in the EHRi

Organisations that share or host components that store PHI must monitor the status and location of media containing unencrypted EHRi data or security critical data, including user registration data, and ensure this data remains physically protected.

SR 71 Robustly Authenticating Users

The EHRi and all POS systems connected to the EHRi must robustly authenticate users.

- The International Organization for Standardization (ISO) called ISO/IEC 17799 "*Code of Practice for Information Security Management."* is a widely adopted international standard already in active use in many Canadian healthcare organisations. The Code begins with a section on how to assess security requirements and how to assess risks and assign controls. One of the 85 security requirements relates to this need to assess the security of a system by using a methodology called threat and risk assessment. The remainder of the Code is organised into eleven sections, each covering a key control area for information security. These eleven information security control areas are:
  - **Information Security Policy**: Each jurisdictional implementation of the interoperable EHR must operate under a security policy appropriate to the jurisdiction and fully adapted to the features of the system that will be operational there.
  - **Organising Information Security:** Five of the security requirements relate to how healthcare organisations manage security and accept managerial responsibility for the security of personal health information. An example is requirement;
    - SR 4 -*Independent Review of Security Policy Implementation*:
    - *Organisations must have the implementation of their information security policy either reviewed independently or attested to in a written declaration by the organisation's chief executive officer or board of directors.*
  - **Information Asset Management:** Three requirements discuss the information assets that must be secured and how they are identified, classified, and handled.
  - **Human Resources Security:** The objective is to reduce the risk of human error, theft, fraud and misuse of facilities. To accomplish this, the system must ensure that users are aware of information security threats and concerns and are adequately trained to be able to support the corporate security policy in the course of their normal work. Also, damage from security incidents and malfunctions caused by human error must be prevented. Six requirements relate to human resources security.
  - **Physical and Environmental Security:** The aims are: to prevent unauthorised access and damage to, as well as other physical interference with, business premises and information; to prevent loss, damage or compromise of assets; to prevent interruption of business activities; and to prevent compromise or theft of information or information processing equipment. These requirements are especially critical in light of recent natural disasters such as Hurricane Katrina. Examples are security requirements;
    - *SR 21-Disposing of or Reusing Equipment:*
    - *All organisations must securely overwrite or else destroy all media containing application software, PHI, or security critical system data when no longer required for use.*
    - *SR 19 – Protecting EHR systems from hazards*
    - *Organisations that share or host components that store PHI must protect sites and equipment supporting the EHRi to reduce the risks from environmental threats and hazards.*

- **Communications and Operational Security:** Operational security: a) ensures the correct and secure operation of information processing facilities; b) minimises the risk of systems failures; c) protects the integrity of software and information; d) maintains the integrity and availability of information processing systems; and e) ensures that the confidentiality, integrity and availability of all data repositories are protected. Communications security aims to protect (principally via encryption) the confidentiality and integrity of every message transmitted from, to, or within the interoperable EHR. These requirements are intended to address security breaches and privacy incidents, such as identity theft, so prevalent in the media. Twenty-nine of the eighty-five security requirements relate to these concerns. Examples include security requirement
  - *SR 31***-** *Encrypting Personal health Information During Transmission*:
  - *Organisations that share or host components that store PHI must apply industry standard cryptographic algorithms and protocols during transmission of PHI to maintain the confidentiality and integrity of this data whenever it is transmitted outside the physical security perimeter that protects information processing facilities supporting servers, applications or data.*
  - *SR 34 Protecting PHI on Portable Media*
  - *Organisations that share or host components that store PHI must ensure that PHI and other security critical data stored on removable media are: a) encrypted while the media are in transit to protect the data's confidentiality and integrity; and protected from theft, where appropriate, while the media are in transit to protect the data's availability.*

- **Access Control:** Access control includes initial registration of users as well as their authentication during log in and their authorisation for access to services and data. Access control is intended to: a) prevent unauthorised access to information systems; b) ensure the protection of services; and c) prevent unauthorised computer access. Twenty-three security requirements relate to access control. Security requirement 61 "*Granting Access By Association*" is one example:
  - *Organisations that share or host components that store PHI a) must be capable of associating users (healthcare providers) with the records of patients/persons and allowing future access based on this association; i.e., they must be capable of granting discretionary access to records based on a registered user with legitimate and pre-existing access to a patient's record(s) granting access rights for that (those) record(s) to another registered user; b)* ***must not*** *allow users to grant other users access to a record if the granting users themselves do not possess such access with respect to the record.*
- **Information Systems Acquisition, Development and Maintenance**: The objective is to ensure security is built into operational systems and to maintain or upgrade the security capability of application system software and of stored data throughout the operational life of the system. Eight security requirements relate to these topics.
- **Security Incident Handling**: Security incident management builds a reporting infrastructure for reporting incidents and weaknesses. It is intended to minimise the damage arising from security incidents and to institute improvements to prevent future occurrences. Two of the security requirements relate to this topic.

- **Business Continuity**: The objective is to prevent or minimise interruptions both to business activities and to critical business processes from the effects of major failures or disasters. Two requirements relate to business continuity.
- **Compliance**: Ultimately, compliance is a jurisdictional concern. Clear policies for compliance audits must be set in each jurisdiction by those who are responsible for governance of the system. This is the only area of privacy or security where Infoway made no attempt to define pan-Canadian minimum requirements.

8. **Openness**

The CSA Model Code states:

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

This privacy principle is closely related to the accountability principle discussed above. The intent is to make it possible for concerned patients to know how their personal health information is collected, used, and disclosed. Privacy oversight bodies (e.g. Information and Privacy Commissioners) may also want assurance that healthcare organisations have privacy management plans in place. One of the 29 EHR privacy requirements relates to openness.

PR 23 Openness

Organisations that share or host components that store PHI must make readily available to the public specific information about their policies and practices relating to the management of PHI.

SR 47 Reporting Every Access To A Patient/Person's EHR

Organisations that share or host components that store PHI must be capable of identifying of all users who have accessed or modified a given patient's/person's record(s) over a given period of time.

SR 48 Reporting Every Access By A User

As well as laying the foundation for the system's privacy and security architecture, the requirements form a highly useful resource for provincial ministries of health that are preparing tenders relating to building such a system. Several provincial ministries of health have indicated their intention to refer to the requirements to reduce the cost of the procurement process. Reference to a common set of requirements not only saves time and money in procurement, but it also helps vendors, who can then design systems that meet one set of requirements rather than many, *must be capable of identifying all patients/persons whose records have been accessed or modified by a given user over a given period of time.*

9. **Individual access**

The CSA Model Code states:

> "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."

Two related privacy requirements contain specific provisions for patient access to personal health information and for the amendment of inaccurate or incomplete information.

PR 24 Patient/Person Access

Organisations must, upon request: a) inform a patient/person of the existence, use and disclosure of his or her PHI and shall give the patient/person direct access to that PHI where such access is not prohibited by legislation; b) respond to requests for access to a patient/person's PHI within a reasonable time and make it available in a form that is generally understandable; and c) allow a patient/person to challenge the accuracy and completeness of his or her PHI and have it amended as appropriate.

PR 25 Amending Inaccurate or Incomplete Information

Organisations should amend PHI when a patient/person successfully demonstrates the inaccuracy or incompleteness of personal health information and notify system users that have accessed the information in question that the information has been amended if the information can reasonably be expected to have an effect on the ongoing treatment of the patient/person.

10. **Challenging compliance:**

The CSA Model Code states:

"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."

The right of any patient to lodge a privacy complaint has been recognised in Canada for decades. Three EHR requirements relate to compliance challenges and complaint investigations.

PR 26 ***C****hallenging Compliance*

Organisations that share or host components that store PHI must give patients/persons the right to address a challenge concerning compliance with these requirements to the designated individual or individuals specified in.policy.

PR 27 Complaint Procedures

Organisations that share or host components that store PHI must a) put easily accessible and simple-to-use procedures in place to receive and respond to complaints or inquiries about their policies and practices and inform complainants and inquirers of the existence of these procedures

PR 28 Investigation

Organisations that share or host components that store PHI must investigate all privacy related complaints. If a complaint is found to be justified, the EHRi, organisations connecting to the EHRi and organisations hosting components of the EHRi should take appropriate measures, including, if necessary, amending their policies and practices and notifying the complainant of actions taken.