Technology Choices and Privacy Policy in Health Care

Medical Informatics Group

Department of Computer Science

Memorial University of Newfoundland

April 2007

Questions regarding this report should be directed to:

Dr. Edward Brown, Associate Professor
Department of Computer Science,
S.J. Carew Building
Memorial University of Newfoundland
St. John's, NL, CANADA A1C 5S7
Tel: (709) 737-7511
Fax: (709) 737-2009
Email: brown@cs.mun.ca

Research Team

Edward Brown, Associate Professor, Department of Computer Science, Memorial University of Newfoundland, St. John's, NL
Harold Wareham, Associate Professor, Department of Computer Science, Memorial University of Newfoundland, St. John's, NL.
Gerard Farrell, Acting Director of e-Health, Faculty of Medicine, Memorial University of Newfoundland, St. John's, NL
Theodore Hoekman, Retired Professor, Faculty of Medicine, Memorial University of Newfoundland, St. John's, NL.
Rhonda Chaytor, Graduate Student, Department of Computer Science, Memorial University of Newfoundland, St. John's, NL.
Jennifer Barrigar, Graduate Student, Faculty of Law, University of Ottawa.
Tracy Ann Kosa, Privacy Assessment Consultant, Toronto, ON.
Carla Barton, Graduate Student, Faculty of Medicine, Memorial University of Newfoundland
Neil Barrett, Graduate Student, Department of Computer Science, Memorial University of Newfoundland, St. John's, NL.
Chris Mercer, Student, Department of Computer Science, Memorial University of Newfoundland, St. John's, NL.
Andree Thoms, Legal Consultant, St. John's, NL.

Acknowledgements

This project was funded through the Contributions Program of the Office of the Privacy Commissioner of Canada, without which the work would not have been completed.

Grateful thanks are extended to those who helped with project resources or otherwise contributed time and effort. The comments, results and opinions expressed in this document are not necessarily reflective of those contributing or participating, and in the spirit of open investigation, this report may not always support the interests or opinions of those contributors. Special thanks go to those who agreed to participate in interviews, most of whom are listed in Appendix A. The report endeavors to accurately represent the opinion of the participants, however, there is always some possibility that the intent of a participant's contribution was not completely captured or that it was used in a context which they would not consider apropos. Apologizes are offered in advance for any errors or inaccuracies that may have appeared.

Additional thanks to: Michael Gurski, Nola Reis, Tim Caulfield, Theresa Scassa, Phillipa Lawson, Bill Pascal, Peggy Blair, Marcel Nouvet, Ian Kerr, Sara Heath, Patricia Kosseim

CONTENTS

Executive Summary

This report examines the relationship between privacy policy and information technology in the health care field. It concentrates on assumptions or biases that available privacy and security technology may be introducing into policy decisions.

This is not an examination of policy process. The focus is in examining how the technology fits with or influences policy as currently expressed in legislation. It does include some attention to the technical, cultural and professional context in which the technology and policy is embedded.

While real progress has been made and possibilities exist for using electronic record systems and applying them to health care, the report content and its interpretation suggest some original policy directions:

Attention should be given to the limitations of strict adherence to a data-protection legislative approach that serves a "security perimeter" model of technology solutions. It is doubtful that a major shift in legislative approach is likely or feasible, but real weaknesses in particular mindsets will only appear if they are adequately critiqued. Part of the critique has to be considering what alternative legislative schemes (addressing both privacy and confidentiality) and technologies to match, might look like, even if political and technical history has already dictated development in a particular direction.

Policy discussion is needed around the question of which rules and procedures will be enforced by technology, which will be monitored by technology, and which will rely on non-technology infrastructure and the ethical and professional responsibility of those in the system. Letting the availability and affordability of security and privacy technology determine their scope or adequacy is ultimately self-defeating, as technology capability is a moving target. Furthermore, there is a risk of creating an illusion of an improved system, as much technology deployment simply shifts the weakest link from one set of humans to another set of humans, and away from the "circle of care".

Finally, policy debate is needed around how trust and confidentiality is expected to be addressed in the new computerized systems. It is not likely that doctors or patients will fully understand the infrastructure protecting their information, the activities undertaken by IT services, or the nature of risks under a technically oriented security and privacy regime. Yet individuals are being required to invest confidence and consent in these mechanisms and the people that maintain them. Not only the corresponding shift in responsibility and professional obligations but also the means by which these things may be exercised in the new environment need to be addressed.

Overview

Part I of the report examines the current state of available privacy and security technology. Technologies are classified into two groups: security technologies, which prevent unauthorized access to data, and privacy technologies, which restrict the actual purposes for which the data is used. There is no generally accepted classification around these technologies. In describing these technologies, privacy and security are often used interchangeably, or the term privacy is sometimes used as a moniker for more complex technology such as trust management or privacy rights management. Alternatively, the more outcomes-oriented term "privacy-*enhancing*" is often used, which is largely independent of specific technology. The division adopted is close to the distinction between data protection (as security) and control of personal information (as privacy) which is developed in Part II of the report.

With cultural and historical seeds in the business environment, these technologies have a strong orientation towards data security, herein called the *perimeter* model. This model's main precepts are to keep away intruders and control inappropriate access. Even the more recent privacy-oriented technologies (such as consent management) are essentially more sophisticated forms of access control. There are some different techniques - malware detection and logging are really surveillance technology - but they can be easily characterized as surveillance *of* the security perimeter.

Whether the perimeter model is culturally or technologically inevitable is not the point. This "business perimeter" orientation creates assumptions about the role of technology in health information privacy. For example, there are no efforts to create technologies for remediation of the effects of a breach on an individual's privacy. Instead, there is a strong orientation to build stronger and stronger security guarantees and detection of breaches, in pursuit of an ultimately unachievable ideal of absolute security, and towards increasingly nuanced and complex versions of the perimeter (such as consent management, trust management and privacy rights management). This is the agenda the technology industry knows how to pursue vigorously.

Within the perimeter model, there are specific cautions about technology choices. Role based access control, consent management and privacy rights management technologies can dictate categories for user roles, types of consent and description of privacy rights in terms of data protection. Engineering these categories is essentially making policy about what data protection choices will be available as well as the information access conditions for the computerized health care system. While good choices may be possible, *defacto* policy created by technology decisions can create a legacy infrastructure that is difficult and expensive to alter in retrospect.

Part II of the report examines the legislative regime concerning privacy and personal health information (PHI). It follows the development of privacy protection in Canada from basic rights provisions, to the operationalization of rights as data protection. Originally designed in response to transborder data flow, rules were instantiated to govern the collection, use and disclosure of personal information. Moved into the private

sector through the federal PIPEDA[1] legislation, these data protection principles became viewed as the means to protect individual integrity and autonomy, as elements of privacy.

The legislative review touches on differences between provinces regarding the patchwork of private and public sector legislation, and difference in rules between jurisdictions. Rather than concentrate on distinctions and harmonization issues, the review turns to jurisdictions that have passed health care specific data protection legislation and examines the influence of technology choices on these laws.

Although nominally technology-neutral, the legislative regime is influenced by existing technology assumptions. As expected, the business-oriented security-perimeter model aligns well with the notion of data protection as a form of privacy. Responding to the imperative to share data in the health world – as a requisite for quality health care – the legislation creates the concept of a custodian/trustee/steward of PHI, and creates rules and procedures for enabling the sharing of data among the custodians. Recognizing that PHI is touched by other roles outside primary care professionals (e.g., IT specialists and companies, administrators, oversight agencies, health surveillance agencies and health researchers) the legislation creates a tangled web of responsibilities through disclosure provisions, patient consent exceptions and agency or contractual relationships that bind others to the obligations of the custodians in a variety of ways.

Two basic questions regarding this paradigm are whether privacy is adequately represented by the notion of the patient controlling their PHI – "informational autonomy", and whether legislative rules and procedures for sharing data really respect this informational autonomy. Assumptions that align well with "business-perimeter" technologies will be opaque under such a regime. Any actual imperative to directly protect privacy as opposed to data – for example, by remediating the effects of a breach on an individual – doesn't seem to enter the legislative frame.

A few pieces of the legislation allude to specific technologies or seem to be predicated on current technology implementations. This ties current legislative policy to accepting particular technological limitations that may disappear in the future, leaving legacy systems that cannot be adequately re-tooled. The other side of this issue is the tendency to leave specific choices and definitions such as "reasonable safeguards" either to operational levels of policy implementation or to IT specialists. Even if acceptable industry norms evolve, this approach may create technological and legislative legacies that are difficult and expensive to alter.

Provisions which purport to extend information autonomy in the guise of data protection may function to restrict it. This includes not only reliance on implied consent or consent exceptions, but the assumption that any consent is meaningfully implemented in technologies like consent management, authorization, privacy rights management or trust management. If the technology deploys consent directives based on roles the patient does not define and implemented in trust management mechanisms from which the patient (or

[1] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

custodian) cannot withdraw trust, the meaning of concepts like trust and consent have been compromised.

Part of this difficulty arises when concepts from technology area, such as the circle of trust and trusted third party, are treated as synonymous with health information concepts, such as the circle of care[2] and custodian. The reality of which party *actually* controls and secures the data may be determined by the technological implementation, not the relationship envisioned by the legislation. For example, the exercise of custody and control over the electronic records relies on those furthest from the circle of care – private companies (IT service providers) – behaving in a trustworthy manner. The intended or legislated relationships may indeed hold, but these obligations are *not* enforced by conventional privacy and security technologies. Some additional enforcement mechanism (or technology) is necessary.

Policy is needed around the question of what the technology will actually enforce or be responsible for. Some current technologies *can* implement disclosure provisions and enforce a perimeter by preventing inappropriate access. Use and collection provisions *could* be monitored through surveillance oriented technologies. However, new infrastructure cannot expand indefinitely, and focusing on these types of technology means alternatives are not pursued.

Part III of the report describes interviews with a number of stakeholders regarding views on the relationship between policy and technology. Informational autonomy is the most cited definition of privacy, but concerns with this concept of privacy as well as limitations to the data protection approach reappear. Personal dignity, confidentiality, and trust and data protection were cited as related to privacy.

The concepts of confidence and confidentiality, barely appearing in the technology or the legislative reviews of Parts I and II, are prominent in the interviews of Part III. The relationship described between confidentiality, data protection, and privacy varied between individuals and appeared to be influenced by the stakeholder's role. One clarification[3] suggests *confidentiality* involves others in protecting shared information, whereas *privacy* involves information under an individual's direct control – each of which is distinct from *data protection*. In practice, those in oversight and policy administration roles tend to engage confidentiality either as incidental to privacy protection, or supporting the basic privacy elements of personal dignity and integrity, through the mechanism of custodial data protection. This is not surprising, as the legislative mandate for oversight and policy administration is limited to data protection. Furthermore, the current technology orientation as noted in Part I directs technology developers towards data protection and information autonomy concepts. The real distinction in interpretation appears with primary care providers.

[2] While not a term in the legislation, "circle of care" is in common use to describe the relationship among care givers, patients and personal health information.

[3] see footnote 357

Privacy is secondary to confidentiality and trust for the physician, or might be portrayed as one result of confidentiality. Physicians hold forthright and specific opinions on the nature, extent, obligations and relationships affecting the confidential exchange of information. Notions like intent and ethical behaviour suddenly appear which are largely outside the language of data protection. Technology and legislation are incidental to competing professional obligations to provide the best care possible and protect the confidentiality of their patient. Technology or legislation that interfere (or are perceived likely to interfere) with professional imperatives may be treated with skepticism and/or circumvented.

Privacy issues are traced back to people. Breaches are attributed to inappropriate internal access or failure of an institution to enforce appropriate access control standards. Exposure to intrusion by outside "hackers" is often portrayed as a fear that is large in the public eye and media, but less of a real threat. The systemic concern is that a breach would result in a failure of public trust. Internal slips or inappropriate browsing by those inside the "circle of care" can be dealt with through institutional responses, without discussing the impact of the breach on the individual. Some policy administrators structure the language around this distinction – external intrusion is a security matter; inappropriate access by those in the circle of care is a privacy matter. This accentuates the business orientation of the technology and institutional process – rules, processes and responses protect the institutional risk which may incidentally protect individual privacy or confidentiality.

Concerns regarding specific technologies are reprised by stakeholders – the risk of aggregate data creating attractive targets for intruders, the immaturity of some security and privacy technologies, limitations of the role-based conception of access control, and whether there is any really meaningful patient control offered through consent mechanisms (both legislative and technological) that are available.

One of the most obvious discrepancies among respondents is the perceived role of policy. One view indicates policy should articulate fair information practices and the proper balance between privacy protection and information sharing appropriate to the health care sector, independent of any particular deployment of technology. Policy may need to adapt to new technology, but basic principles remain the same. The opposite view is driven from practical experience that existing policy simply does not provide the specific advice to make technology choices, the very choices that affect confidentiality, trust and privacy outcomes. This cannot be simply discounted as the difference between high level legislative policy and its interpretation at the administrative or operational level. The fact that these choices are made independently in different locations or different jurisdictions at the operational level is part of the concern. Harmonizing these choices is not a job to be left to IT personnel.

Traditional elements of confidentiality and trust are transformed by the legislation and technology of the computerized health care system. Instead of trusting the care provider to keep a confidence, the patient must now place their trust to the computerized security and privacy mechanisms which are increasingly out of the care provider's hands. Likewise, care providers must trust their professional obligations to these same

mechanisms. This trust may extend even further – to the policy administrators, IT maintenance and service personnel in charge of the technology. The very authentication and consent management schemes designed to give us confidence may in fact send a very different message: that those in the circle of care are no longer to be trusted to behave appropriately, but must be monitored and controlled by technology.

Part I: Privacy-Related Technologies: An Overview

1 Introduction

The central theme of the report is examination of the relationship between privacy-related technologies and health information policy. This first phase of the report introduces privacy related technologies, their strengths, weaknesses and possible application in health care context.

While the use of electronic information systems has a long history of steady growth in health care as in all sectors, two federal initiatives in particular have pushed the relationship between health care information and privacy to the forefront.

In 1999, the final report of the federal Advisory Council on Health Infostructure (ACHI)[4] recommended a significant investment in a pan-Canadian health information system. This report laid out a comprehensive vision of improving the quality, accessibility, portability and efficiency of health services along with ways to give Canadians greater control over their health through access to better information. The central idea was "seamless delivery of patient care from one institution to another and from one geographic area to another."

About the same time a new data privacy regime was taking shape around the CSA model privacy code, incorporated in federal legislation in 2001 as the *Protection of Personal Information and Electronic Documents Act* (PIPEDA). Centered on the theme of consent for the collection, use and disclosure of personal information, this code presented some difficulties for the conventional exchange of data within a health information system. Respecting privacy while maximizing benefits from the information-sharing capabilities of an electronic health information system is a difficult balancing act.

Following the ACHI report, Canada Health Infoway was created in 2001, carrying a mandate to promote the development of electronic health information systems in Canada. Privacy protection was recognized as an important element of this effort:

> A key foundation of the Canada Health Infoway will be achieving greater consistency and harmonization of provincial, territorial and federal privacy legislation for privacy protection in the health sector. The implementation of fair information practices and privacy-enhancing technologies throughout the health sector will also be a priority. While enabling patients to access critical information in their health records, 24 hours-a-day, seven days-a-week, this system will involve strict and explicit controls. There will be fuller assurance of confidentiality than can be provided today with a paper-based system. The Canada Health Infoway will also permit quick access to personal medical

[4] Advisory Council on Health Infrastructure (1999) Final Report. Available online: http://www.hc-sc.gc.ca/ahc-asc/media/nr-cp/1999/1999_16_e.html

histories by health care professionals and providers on a need-to-know basis. This will ensure safe, effective treatment while avoiding expensive, unnecessary and sometimes risky tests.[5]

While it would be wrong to characterize Canada Health Infoway as the originator of electronic health systems (as many jurisdictions in Canada have both systems and legislation in place prior to 2001), the emphasis it has placed on interoperability of health information systems, and a 2009 timeline for achieving substantial connectivity of such systems, has encouraged rapid development of working systems.

Figure 1 is meant as a conceptual diagram for how a networked health care system might appear for the purposes of understanding the information technology components. The diagram is deliberately vague with respect to physical structure, due to the variety of possible arrangements of data infrastructure, networks, and individuals with different roles in the system. It does help identify some common terms, however.

Terms such as personal health record, electronic health record and electronic medical record, electronic patient record, e-Health are often used interchangeably in different contexts. For the purposes of this report, certain distinctions are maintained:

- The term **electronic health record (EHR)** is used for an institution-wide or cross-institution record which accumulates health information about an individual. Conceptually, this is massed information about the individual which may originate from different health care services or information sources. Typical institutional concerns may not necessarily be limited to primary care delivery activities: for example, accounting, payroll, administration may be incorporated into a hospital's EHR. In dealing with strictly administrative activities, the term *health management system* is preferred; however, it is important to note these functions may be integrated with an EHR.

- The term **electronic medical record (EMR)** is used more specifically to refer to information tools used at the point of primary care delivery: an electronic record maintained for a clinic, for example. This sort of information tool may be considered as supporting a physician's (or other provider) care of their patient. Roughly, it is an analogue to the patient record in a physician's office, except that the data may be stored with or linked to other systems. One would expect most health care providers' point of contact with the system to be through an EMR.

- The term **personal health record (PHR)** is used to describe the patient's ability to manage their health information directly. Conceptually, the individual might examine their health reports, billing, and scheduling along with utilities for tracking their personal lifestyle choices such as exercise and diet. The ability of the individual to manage their personal health information (PHI) might include

[5] see footnote 4.

the ability to observe their clinical or hospital records. Such PHR systems might be provided through web browser access, for example.

- the term **health-record system** is used to refer collectively to all three types of records and their associated application softwares.

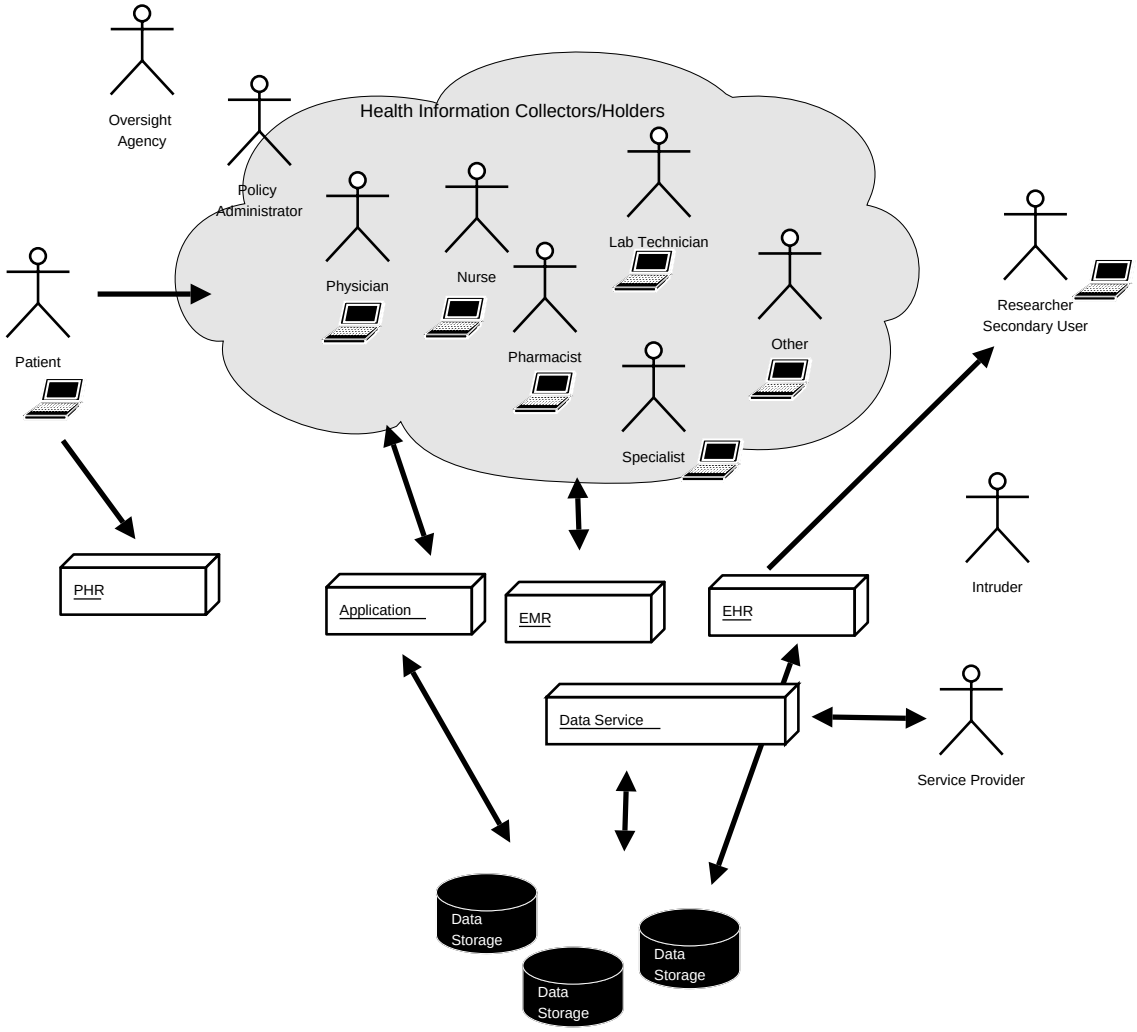

Figure 1: A Generic Computerized Healthcare System.

The relationship between electronic record systems can vary: the EMR might consult an EHR to obtain missing information, or vice versa, for example. The cloud of health information collectors and holders in the diagram is meant to indicate those associated with primary care delivery or working in support of primary care. Outside this cloud of actors are the potential intruder, the oversight agency (which could be a privacy official, or a health or state agency which ensure the rules are observed) and the secondary user - someone that has access to the data for a secondary (non-primary care) purpose. Examples of secondary use are public health surveillance and health research.

The service provider is an important role in the Figure. He highlights the fact that some component of the system infrastructure will typically exist outside the traditional health

care system, maintained by a separate (probably private sector) entity - the service provider. While hospitals may house their own services and technology, with their own IT and computer support staff, the power of networking is that data and services can be shared and housed remotely. Furthermore, these services can be configured in many different ways - portions of a patient record may be stored and served remotely while other portions may be local. The service provided may be something different than the data records as well; patient registries, security services or privacy services are all possibilities that may or may not include storage and maintenance of personal health information (and non-health personal information). Provision of such services is often seen as requiring special expertise, or cost benefit savings, that can be obtained by going outside the health care institution.

An EHR or EMR might be idealized as a comprehensive information solution for a clinic or institution; but it might not. It could as easily be an amalgam of distributed data services and applications. Other applications and features may be added as new technology becomes available; and the technology in use is often a collection of tools rather than a single solution. For example, most organizations will see at least some relevant information relayed through an email service, regardless of what specialized applications are available. Furthermore, the relationship among the components of Figure 1 is not a fixed relationship: an EHR may draw information from an EMR or vice-versa; each of these may get information from a variety of data services, which may share them with other applications and/or institutions.

The next section of this report attempts to place ***privacy-related technologies*** with respect to these components. The more conventional term *privacy-enhancing technologies (PETs)* is avoided because that term relates more to the context of a technology application than to a particular technique. For example, the use of email rather than faxes may be termed privacy-enhancing in a particular context. In fact, these applications do raise important privacy concerns, and an organization's privacy officer or risk assessment officer may spend a great deal of effort determining how to use particular applications in secure and privacy-enhanced manner. This report, however, looks at technologies particularly designed for security and privacy purposes.

2 Privacy-Related Technologies

This section describes various technologies used to address privacy concerns in electronic information systems. Because of this focus, many technologies that may be familiar are not extensively treated: it is not the objective to explain how the internet or web browsing functions, for example. Many ubiquitious security components, such as passwords, firewalls or virus blockers, are treated in the context of a more general category of techniques, since the main effort is to explain some of the current and forward-looking technologies that may be candidates for adoption now or in the near future.

Each technology will be described in terms of the following four characteristics:

- **Risks Addressed** - The particular risks that motivate (and are hopefully dealt with) by this technology. Generally, these are related to data security or privacy.

- **Where It Occurs** - The places in a computerized healthcare system (such as a database) where this technology is typically implemented. This is phrased relative to a general possible model of a computerized healthcare system (see Figure 1).

- **What It Does** - The manner in which this technology operates.

- **Limitations and Concerns** - Limitations and potential problems associated with the use of this technology.

These technologies are broken into two main groups, based on whether a technology primarily deals with security (Section 2.2) or privacy (Section 2.3). As many of these technologies are based on fundamental cryptographic technologies, these cryptography-based technologies are described first in Section 2.1 .

Security and privacy are frequently confused, or these terms are used with different connotations or intent. In subsequent parts of this report, the relationship between privacy and data protection will be scrutinized from several perspectives. For the purposes of this part, it is only necessary to distinguish two types of technology, based on the intended application of the technology.

As a category, security technologies ensure that data is protected so that only authorized users have access to that data. In other words, it is a matter of keeping the data safe from outsiders. The privacy category encompasses technologies for ensuring that the individuals or organizations described by that data will not have "their" data put to unauthorized use; possibly involving (where appropriate) some degree of control over the manner in which "their" data is disclosed and used.

Under these definitions, it is clear that security is a prerequisite for privacy; and furthermore, security itself is not privacy. Imagine an organization that stores data on individuals in a locked underground vault and grants access to this data to the highest bidder, who may then use this data as it pleases. Such a system is definitely secure yet equally definitely violates the privacy of the individuals described by the data.

2.1 Cryptography-Based Technologies

Encryption is fundamental to computer security, be it secure e-mail messages, encrypted databases or hard drives, or other technology. The three technologies described in this section build upon one another - digital signatures (Section 2.1.2) are created using two-key cryptography (Section 2.1.1), and public-key-based certificate infrastructures (Section 2.1.3) use both digital signatures and two-key cryptography. Table 1 shows which cryptography-based technologies are required to build each of the security and privacy technologies subsequently described in Sections 2.2 and 2.3 .

Technology	Text	1-KC	2-KC	DS	PKI
User Authentication	2.2.1	-	✓	✓	✓
User Authorization	2.2.2	-	✓	✓	✓
Activity Logging and Auditing	2.2.3	-	-	-	-
Intrusion and Malware Detection	2.2.4	-	-	-	-
Data Encryption	2.2.5	✓	✓	-	-
Data Authentication	2.2.6	-	✓	✓	-
Secure Remote Access	2.2.7	✓	✓	-	✓
Trust Management	2.2.8	-	✓	✓	✓
Data Storage Management	2.2.9	✓	✓	-	-
User Identity Management	2.3.1	-	✓	✓	✓
Data Anonymization	2.3.2	-	-	-	-
Privacy-Preserving Data Analysis	2.3.3	-	-	-	-
Consent Management	2.3.4	-	✓	✓	✓
Privacy Rights Management	2.3.5	-	✓	✓	✓

Table 1: Cryptography-techniques used in Security and Privacy Technologies.

2.1.1 Single-key and Two-key Cryptography [6]

What It Does: All cryptography technologies protect data by transforming it into a form that is only readable to those who are authorized to work with that data. During encryption, a given piece of data called the *plaintext* is transformed into a different piece of data called the ***ciphertext***. For example, if a Doctor's prescription is the plaintext, the prescription data could be encrypted into un-readable cyphertext before being emailed to a pharmacist. This transformation is specified by a piece of data called the *encryption key*. It should be difficult to extract data from the ciphertext without access to the appropriate ***decryption key***, a piece of data that allows the ciphertext to be decoded to

[6] Bragg, R. (2004b) "Data Security Architecture." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) *Network Security: The Complete Reference*. McGraw-Hill / Osborne; New York. 153–174.

reproduce the original plaintext. In our example, the pharmacist would have to decrypt the cyphertext back into a plaintext prescription to read it.

There are two types of encryption schemes. In single-key cryptography, the encryption and decryption keys for a particular plaintext are the same. In two-key cryptography, these keys are separate and you cannot derive one from the other. There are many fast single-key encryption schemes available; however, as there is only one key, this key has to be kept secret to protect any ciphertexts it has been used to create (this is why single-key schemes are also called *secret-key cryptography*). Two-key encryption schemes tend to be much slower than single-key schemes; however, as there are separate encryption and decryption keys, there is now the option to make one of these keys public and keep the other one private (which is why two-key schemes are also called ***public-key cryptography***). This allows two possible situations:

- **Encryption key public / Decryption key private**: Anyone can encrypt messages, and these messages can only be decrypted and read by the owner of the decryption key.

- **Encryption key private / Decryption key public**: The owner of the encryption key can create messages that can be decrypted and read by anyone.

The first situation allows for secure communication over communication networks - if the two people who wish to communicate both have public encryption keys, they can send messages to each other that no one else can read, even if these encrypted messages are intercepted. As described below, both situations have many uses in various security and privacy technologies.

Limitations and Concerns: The weakest point in any cryptographic technology is the keys. Given the careless manner in which many people treat other crucial pieces of data such as passwords or ID cards, this would seem to be serious. However, most encryption is done automatically – for example, when you visit a secure web site, you don't have to remember an encryption key for the web site, it is done automatically, taking advantage of secure key-sharing technologies similar to the PKI mechanism described below. As a consequence, human carelessness is not as prolific a problem it might first appear to be.

Potentially greater though less obvious concern is the fact that any encryption scheme can be broken - with enough computing power and sufficient amounts of ciphertext, keys can be discovered or ciphertext can even be decrypted without keys. One way of getting around this is to change keys frequently – an approach used by applications that send messages across the internet typically will employ this approach, using a different key for each message. A more general solution is to use an encryption scheme that makes such attacks as computationally expensive as possible, by using either a computationally complex scheme or large encryption and decryption keys. Encryption schemes have a wide variety of attack-costs, and the appropriate encryption technique or should be chosen for the task at hand.

2.1.2 Digital Signature [7]

What It Does: A digital signature attached to an electronically-stored piece of data does the same thing that a handwritten signature does for a paper document - that it, it shows that this data was created by a particular person. Digital signatures can be created using public-key cryptography. A person who creates and wishes to sign a piece of data (call him the signer) obtains a key-pair, and makes the decryption key public. To sign a piece of data, the signer creates a simplified form of the data called a ***digest*** using some standard publicly-known method, encrypts that digest, and attaches it to the data (which is not encrypted) as a signature. Anyone can now verify that this data-signature pair is in fact from the signer by creating a digest of the unencrypted data and comparing it against the decrypted signature - if the digest created by the verifier and the decrypted signature are identical, the only person who could have created that data is the signer. The obvious application in the health care setting is to prevent forged electronic documents, such as prescriptions or lab reports.

Limitations and Concerns: It is crucial that the encryption key be kept private - otherwise, anyone who obtains that key can now create fake signatures.

2.1.3 Public-key-based Certificate Infrastructure [8]

What It Does: Many applications that use public-key cryptography require that the identity of the person or organization using a particular key be attached in some fashion to that key. For example, in an on-line sale being negotiated using public-key cryptography along the lines sketched in Section 2.1.1 , the buyer needs to know who the seller is and vice versa. A piece of data that describes an identity and its associated public key is called a ***certificate***. Certificates can have expiry dates attached to them; this is convenient if a particular key or identity is only valid for a particular length of time, such as the period in which a buyer can return a purchased item or the time until a student graduates from a university and stops having lending privileges at the university library.

Certificate infrastructures allow users to create and work with certificates in a reliable way. As such infrastructures are typically based on public-key cryptography, they are often called ***Public-Key Infrastructures (PKI)***. To help users ensure that they only work with certificates that are valid, certificates are issued by trusted third parties called ***Certificate Authorities (CA)***. A CA attaches its own digital signature to any certificate that it issues. To use a certificate, a user does the following:

1. See if that CA is trustworthy
2. Check the digital signature to make sure that the CA actually did issue the certificate; and
3. Check that the certificate is still valid.

[7] Akl, S.G. (1983) "Digital signatures: A tutorial survey." *IEEE Computer*, 16(2), 15–24.
[8] Adams, C. and Lloyd, S. (2003) Understanding *PKI: Concepts, Standards, and Deployment* (Second Edition). Addison-Wesley; Reading, MA.

Additional information may also be attached to certificates, creating different types of certificate infrastructures. For example, the different ways that a user may be authorized to access a particular computer system may be attached to that user's certificate, yielding certificates that are dealt with by a ***Privilege Management Infrastructure (PMI)*** .[9, 10] Given these different types of infrastructures, the term PKI is restricted to infrastructures that only use basic identity-key certificates.

Limitations and Concerns: As certificate infrastructures are based on both public-key cryptography and digital signatures, they inherit all problems associated with these technologies. Many additional problems arise from how various operations described above are implemented in an infrastructure.[11, 12] For examples,

- There are typically many CAs in an infrastructure, and these CAs can issue certificates for and hence validate the actions of other CAs. Assessing whether a CA is trustworthy involves finding a chain of CA-validations linking the CA issuing a certificate of interest to a CA that a user trusts, which is hard to do efficiently. As a result, step #1 is often skipped.

- The number of expired and known fake certificates typically becomes very large very fast. Current schemes for checking certificate validity either download a list of revoked certificates (*Certificate Revocation List*) from the CA for the user to check or ask the CA to check its own revoked certificate list; both are hard to do efficiently.

Ongoing work is developing techniques to fix many of these problems.[13, 14] However, the most critical problem is that public-key certificate infrastructures are often mis-used - they work best doing what they were designed to do (linking public keys to identities) and have proven less reliable when applied to tasks such as privilege management. The exaggerated claims of reliability and/or functionality by companies mis-using these infrastructures, and the mishaps arising when the infrastructures malfunction, has in turn generated an underlying distrust of certificate infrastructures in general. This distrust could be a barrier to widespread use in a field such as healthcare.

---

[9] Blobel, B. *et al*. (2003) "Using a privilege management infrastructure for secure web-based e-health applications." *Computer Communications*, 26, 1863–1872.

[10] Chadwick, D. (2004) "The X.509 Privilege Management Infrastructure." In Jerman-Blažič, B., Schneider, W., and Klobučar, T. (eds.) (2004) *Security and Privacy in Advanced Networking Technologies*. NATO Science Series III: Computer and Systems Science – Vol. 193. IOS Press; Amsterdam. 15–25.

[11] Clarke, R. (2000) *Conventional Public Key Infrastructure: An Artefact Ill-Fitted to the Needs of the Information Society*. Technical Report. Available online: http://www.anu.edu.au/people/Roger. Clarke/II/PKIMisFit.html.

[12] Ellsion, C. and Schneier, B. (2000) "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure." *Computer Security Journal*, XVI(1), 1–8.

[13] Adams, C. and Just, M. (2004) "PKI: Ten Years Later." In *Proceedings of the 3rd Annual PKI R&D Workshop*. 69–84.

[14] Gutman, P. (2002) "PKI: It's Not Dead, Just Resting." *IEEE Computer*, 35(8), 41–49.

2.2 Security Technologies

2.2.1 User Authentication [15]

Risks Addressed: User authentication prevents unauthorized users from reading or manipulating data. By giving authorized users a way of verifying their identity, it difficult for unauthorized users to access data using regular system-access routes.

Where It Occurs: Any data store or application that has an associated list of authorized users can, when dealing with a user request, ask for that user to identify themselves and hence confirm that they are authorized. For example, if a nurse requests the current drug prescriptions of a patient in a particular ward in a hospital, the EMR may require that nurse to confirm that this patient is under her care; similar confirmation may be required of doctor prescribing a chemotherapy regimen for a cancer patient.

In addition to granting authorization, user authentication is also part of many auditing processes,[16] as it indicates exactly who performed (and hence may be responsible for) a particular action. For example, it is not only important that a doctor be authorized to prescribe chemotherapy for a cancer patient, but that this doctor's name be recorded on that prescription so that he or she can be consulted if problems arise when that regimen is given to the patient.

User authentication is a critical component of all health-record systems (EMR/ EHR/ PHR), applications, data services, and individual user computer systems within a computerized health care system (see Figure 1). At present, user authentication is typically done by each software application individually and is not contracted out to a data service. However, in certain situations such contracting could be preferable. For example, when a group of closely-related software applications are dealing with many users who have multiple on-line identities, a common user authentication service makes sense. (see Section 2.3.1).

What It Does: User authentication technologies establish the validity of a claimed user identity. Traditionally, this has been done by issuing a unique username-password pair to each authorized user (a single password may also suffice, as long as it is unique to a user). When a system request is made, the user also enters this pair to confirm identity and hence authorization. This has been simplified with smart cards; the user need no longer remember a username and password, but need only present the card to a card reader when making a request. A variant on smart cards implants this information within the user encoded in radio-frequency identification (RFID) chips that are placed under the skin. In both of these cases, the identifying information encoded in the card or RFID may

[15] Bragg, R. (2004a) "Authentication and Authorization Controls." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) *Network Security: The Complete Reference*. McGraw-Hill / Osborne; New York. 127–152.

[16] Bragg, R. (2004c) "Security Management Architecture." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) *Network Security: The Complete Reference*. McGraw-Hill / Osborne; New York. 175–190.

be a PKI certificate. Biometric technologies promise even simpler user identification through the ability to scan and hence identify users by personal body characteristics, such as fingerprints or retinal blood-vessel patterns.

Limitations and Concerns: Ideally, any kind of information used for user authentication should satisfy three properties:

1. it should be physically associated with the user;
2. it should be reliably readable for authentication;
3. it should be complex enough that it cannot be forged, duplicated, or guessed by so-called "dictionary attacks", in which all combinations of simple and/or easily-guessed identification information are applied to force improper authentication.

Every known technology fails one or more of these properties. Username-password schemes are notoriously easy to subvert, in large part due to bad user habits that range from leaving written records of passwords adjacent to computer terminals to changing passwords to easily memorable variants such as "AAA111" (violations of (1) and (3)). The underlying problem is that people don't want to or can't remember assigned passwords; typical solutions such as issuing multiple passwords or changing passwords frequently only make things worse. Smart-card based authentication schemes including RFIDs address human memory difficulties. However, smart cards may still be stolen and it is surprisingly easy to duplicate (and hence forge) the identification information stored on smart cards and RFIDs [17] (violations of (1) and (3)). At present, biometric schemes seem the most promising; however, current scan technology is not yet 100% accurate and it is not yet known how easy it will be to forge biometric characteristics (violations of (2) and possibly (3)).[18]

2.2.2 User Authorization [19]

Risks Addressed: User authorization prevents valid users of a system from accessing (either accidentally or on purpose) data and data manipulation functions for which they are not authorized.

Where It Occurs: It is seldom the case that an authorized user for a data store or application is allowed to access all data or data manipulation functions; there are usually restrictions, some imposed by the role of the user in the organization and others by the order of other people. For example, a nurse could have restricted EMR access to the medical records of patients currently under her care, a medical lab technician could be restricted from the ward and chart ID of the patient whose samples they are processing,

[17] Kerr, I. (2006) "Health Chips? Using Implanatable RFID to link Patients to Health Records." Talk presented at the 2006 Electronic Health Information & Privacy (EHIP) Conference. Available online: http://www.ehealthinformation.ca/documents/EHIP2006.pdf

[18] Matyáš, V. and Riha, Z. (2004) "On the Usability (and Security) of Biometric Authentication Systems." In Jerman-Blažič, B., Schneider, W., and Klobučar, T. (eds.) (2004) *Security and Privacy in Advanced Networking Technologies*. NATO Science Series III: Computer and Systems Science – Vol. 193. IOS Press; Amsterdam. 178–190.

[19] see footnote 15.

and a doctor prescribing chemotherapy could be restricted to ordering only cancer-related surgical procedures.

User authorization has potential value for all health-record systems, applications, data services, and individual user computer systems within a computerized health care system (see Figure 1). At present, user authorization is done by each software system individually and is not contracted out to a data service; however, if proposed trust and consent management technologies become widespread, they will likely have to work across multiple systems and user authorization would be a candidate for separate servicing. (see Sections 2.2.6 and 2.3.4).

What It Does: User authorization technologies associate sets of authorized data and data manipulation access-permissions with each user, and these permissions are enforced whenever a user is authenticated for system access. These permissions can be stored on system-specific lists or user-specific PMI certificates (see Section 2.1.3). Many database systems allow remarkably fine-grained restrictions on the particular database records and fields within those records that the user is allowed to view and/or manipulate. Permission-sets can be built individually for each user, but this is time-consuming and prone to error. The more common approach is to associate each user with one or more roles in the system, ands associate a standard permission-set with each role (***Role-Based Access Control (RBAC)***). These roles can be based on the roles of users within organizations (such as hospital administrators, doctors, nurses, and researchers), the relationships of users to the people described in the data (such as doctors and nurses to patients under their care), or the geographical locations of users.

Limitations and Concerns: Proper user authorization depends on proper user authentication, and hence inherits all the problems described in Section 2.2.1 . As well, there are many potential problems inherent in any user authorization scheme. Maintaining the proper permission-sets for large numbers of users is a complex undertaking and prone to human error on the part of permission-set administrators, often leading to users having access privileges they never should have been granted; the additional permissions made possible by fine-grain access controls within current database systems only makes this worse. Difficulties also arise when a user has several associated permission-sets and some of theses permissions and restrictions contradict each other. For example, a doctor who is temporarily assigned administrative duties may be allowed to look at the EMR record of a patient under her care (as that patient's doctor) but be forbidden from looking at the test results associated with any patient (as an administrator). Such situations can be resolved automatically using rules, but coding rules that are error-free and able to handle all possible situations (let alone handle these situations correctly) is very difficult.

2.2.3 Activity Logging and Auditing [20]

Risks Addressed: Activity logging and auditing records reading or manipulating of data or system operation. Through surveillance of unauthorized activity, steps can then be taken to stop ongoing activity, repair any damage done, and prevent future activity.

Where It Occurs: A computer system user is any individual person or computational process that interacts in some manner with that system. This activity can take the form of activating some function of the system (including system access) or accessing or manipulating particular pieces of data stored on a system. For example, a nurse may request a monthly report on a particular ward, a doctor may want to read and then update the chart of one of her patients, or a chemotherapy prescription system may automatically send out the daily order of prescribed drugs for and update the treatment-regimen progress chart of a cancer patient. This user activity may be authorized or unauthorized, and one way of detecting unauthorized user activity is to keep track of the activities of all users in special log files and examine (***audit***) these log files for patterns indicative of unauthorized use.

Activity logging and auditing might occur for any health-record systems, applications, data services, and individual user computer systems within a computerized health care system (see Figure 1). This could apply to both the software and hardware components. Logging is typically done by individual components or applications, though logs may be consolidated into master log files to make the auditing process easier.

What It Does: Activity logging technologies arrange for information about activity of particular hardware or software to be stored in a special log file. Typically the identity of the user and the nature of the activity are recorded. An arbitrarily detailed description could in theory be stored; however, given the speed with which activity-events occur and hence their sheer numbers, the required log-file space would be impractical. Hence, only the most relevant information is typically stored. In certain situations, further log-file space may be saved by storing a compressed description of the activity-event that can be expanded (at some computational cost) if the activity-event is examined. For example, in the Hippocratic Database System, full lists of all records accessed and/or modified by a particular database query are not kept – rather, the sequence of query-events is saved, and the accessed-records list can be reconstructed from this query-event sequence as necessary during auditing.[21]

Auditing technologies automatically generate summaries of overall system activity from associated log files for perusal by human systems personnel. Though such summaries may give indications that certain types of unauthorized user activity may be taking place, the actual detection and characterization of such activity is done by intrusion and malware detection technologies (see Section 2.2.4).

[20] see footnote 16.

[21] Agrawal, R., Garndison, T., Johnson, C., and Kiernan, J. (2007) "Enabling the 21st Century Health Care Information Technology Revolution." Communications of the ACM, 50(2), 35–42.

Limitations and Concerns: Correct logging of user activity-events depends on proper user authentication, and hence inherits all the problems described in Section 2.2.1 . As the identities of computational processes can be disguised in many of the same ways as human user identities, correct logging of process activity-events is subject to many of the same problems. The log-files themselves also pose several problems: the space required to store such files may be practically prohibitive even for moderate levels of user activity; the files may be misleading, *e.g.*, portions of the master system log may become lost or altered during consolidation; and, given that such log-files can be examined to reconstruct the activities of individual users (even authorized ones), they are another form of personal (and hence private) information, and must be protected from unauthorized use just as rigorously as other stored personal information on the system.

2.2.4 Intrusion and Malware Detection [22, 23]

Risks Addressed: Intrusion and malware detection stops unauthorized users from reading or manipulating data or interfering with regular system operation, either by system access or by running unauthorized software (***malware***) within the system. By detecting such unauthorized activity, steps can be taken to stop ongoing activity, repair some kinds of damage, and prevent future activity.

Where It Occurs: All computerized data stores and applications run on computer systems which interact via communication networks. Intrusion can take place both through regular system-access routes (by an intruder attempting to gain access with a collection of typical usernames and passwords) or by tapping into the underlying network software or hardware. Malware can placed within any computer system involving software, either by a human being putting it there or malware copying and spreading itself along communication networks to other systems. Commonly-encountered types of malware are computer viruses and worms, which wreck havoc by propagating in an uncontrolled fashion over computer networks, and spyware, which monitors and reports on private system activity (such as username and password entry) to an intruder.

Intrusion and malware detection belong in all health-record systems, applications, data services, and individual user computer systems within a computerized health care system (see Figure 1). At present, intrusion and malware detection is the separate responsibility of each of these components. It is becoming more frequent (especially in the case of smaller subsystems that cannot afford the expense of dedicated personnel to operate these technologies) to outsource the more basic intrusion and malware detection services to

[22] Debar, H. (2004) "Intrusion Detection Systems – Introduction to Intrusion Detection Analysis." In Jerman-Blažič, B., Schneider, W., and Klobučar, T. (eds.) (2004) *Security and Privacy in Advanced Networking Technologies*. NATO Science Series III: Computer and Systems Science – Vol. 193. IOS Press; Amsterdam. 161–177.

[23] Grimes, R.A. (2004) "Intrusion-Detection Systems." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) *Network Security: The Complete Reference*. McGraw-Hill / Osborne; New York. 295–334.

trusted third parties.[24] Given sufficient advances in artificial intelligence technologies, it conceivable that all such services may in time be done by automated data services.

What It Does: Both intrusion and malware detection technologies rely on system activity auditing technologies which maintain log files containing dates, times, and (where known) users responsible for various system activities of interest such as system access, data access, and data modifications.[25] These logs are scanned, either for significant differences from normal system operation (***anomaly detection***) or particular patterns that are characteristic of known intrusion methods (***signature detection***). For example, an unusually large number of unsuccessful password-access attempts within 5 minutes in the middle of the night or a smaller but regular cycling in the number of such attempts over a several week period may be indicative of a dictionary attack on the system; similarly, an unusually large or cyclic number of outgoing messages to random connected systems may be indicative of a computer virus or worm attack. Such scans may also pick up unauthorized or accidental activities by legal users of the system. In the case of malware, individual files in a system as well as incoming messages from networks may be scanned to detect bit-patterns corresponding to all or part of the code making up known malware threats.

The detection of anomalies requires models of normal system operation, which can be derived by machine learning algorithms during a training period of regular system operation. The detection of signatures requires access to databases of known threat signatures. Detection can be done continuously; however, given the long duration of certain intrusion activities and the cost of continuously scanning system activity and/or files, detection is often done at fixed times such as every 6 hours.

Limitations and Concerns: The additional storage required by log files may be practically prohibitive, even for moderate levels of activity detail. Moreover, there are additional problems particular to both anomaly and signature detection. Signature detection only works for known threats. Though there are a number of on-line databases of known malware signatures that are updated frequently, new malware is always emerging and it is inevitable that some damage may occur before a new threat is recognized. In theory, anomaly detection can deal with such situations; however, intrusion and malware can be adjusted to behave very similarly to authorized software. The amounts of system activity data that must be processed to build a model that reliably distinguishes authorized from unauthorized behavior may be prohibitive, as may the computational expense of deriving this model. One solution is to use less data and effort to derive a less sensitive model; however, such a model typically generates a large number of unnecessary alarms for legal system activity that is judged suspicious (false positives) and may fail to detect actual threats (false negatives), both of which make anomaly detection much less useful.

[24]Himmelsbach, V. (2006) "When and why should you outsource your security function to a managed provider?" *Technology in Government*, 13(5), 8–11.
[25]see footnote 16.

2.2.5 Data Encryption [26]

Risks Addressed: Encryption prevents the reading of data obtained by unauthorized means or by unauthorized persons. By creating an encrypted version of given data called a ciphertext with the aid of an encryption key, it can be made difficult for anyone to understand the data without the aid of the appropriate decryption key.

Where It Occurs: Data may be held in storage in an encrypted fashion, and only decrypted when it is actually used. For example, if a physician is using an EMR and the EMR stores data on a hard drive, the data may be encrypted and decrypted as it is placed on and removed from the drive. If the hard drive is stolen or the device inadvertently removed, it will be difficult for others to read the data without the appropriate decryption key. Data may also be encrypted for transmission over the internet or other network use. This can help protect the data during transmission. For example, if a lab is sending records to a hospital, encryption could help prevent data theft by malicious intruders or inadvertently sending data to the wrong address. Both of these types of encryption are typically done automatically by the software programs involved, which keep track of the various encryption and decryption keys so that users don't have to remember them.

Data encryption is a suggested component of all health-record systems as well as communications between these systems and all other applications within a computerized health care system (see Figure 1). At present, data encryption is done by each health-record system individually, and given the need to protect as much as possible the associated encryption and decryption keys, it seems unlikely that this can ever be contracted out to a data service. However, the integration of data encryption schemes into data storage hardware (such that all data stored on such hardware is automatically encrypted and decrypted as it enters and leaves storage) and standard software solutions means that data encryption is easily included in data and communications systems.

What It Does: Encryption is most efficiently done using single-key cryptography. It is easy to apply this to stored data, where the entity that controls the data both encrypts and decrypts data as necessary. Potential problems arise for transmitted data, in which the encrypting transmitter and decrypting receiver are physically separated. Traditionally, any such key would be passed between the transmitter and receiver over the telephone or in person; however, such schemes are impractical when these keys are used to encode large numbers of automatically- and rapidly-issued messages. In such situations, public-key cryptography can be used to share a single-key encryption key - this is done by the transmitter encrypting a generated key using the receiver's public encryption key, which can be sent over insecure transmission lines only to be recovered using the receiver's private encryption key.

The simplest applications of encryption treat an entire record as a plaintext. This is acceptable if an authorized user is allowed to look at entire records. This might be the case for nurses and doctors, who should be able to see the entire medical records in an

[26] see footnote 6.

EHR of patients under their care. However, there are many applications in which users may only be authorized to look at particular portions of records. For example, technicians in a medical testing lab may only be allowed to know chart numbers and sample identification codes instead of a patient's full name and address. In such applications, the sensitive portion of a record can be treated as the plaintext, or a record can be broken into several plaintexts that are encrypted and decrypted by their own sets of keys particular to the users authorized to access those portions of the record.

The examples above show that possessing the decryption key for a piece of data might be treated the same as having permission to look at and manipulate that data. Sometimes, the permission of several individuals or groups may be required to access a piece of data. For example, a consulting specialist may only be allowed to look at a patient's record if both the patient and that patient's family doctor give permission. One way of dealing with this is to split the decryption key into several pieces that are distributed among the permitting parties. Alternatively, data can be encrypted several times in a particular order, using encryptions keys owned by and specific to each of the permitting parties. Such data can only then be recovered by applying all of the appropriate decryption keys in the reverse order.

Limitations and Concerns: Data encryption inherits all the problems and limitations associated with secret- and public-key cryptography and PKI. Additional problems arise with maintaining keys for data stored in long-term archives (see Section 2.2.7).

2.2.6 Data Authentication [27]

Risks Addressed: Data authentication prevents both authorized and unauthorized users from either modifying data belonging to by others or claiming that a piece of data belonging to them does not belong to them. By assigning a digital signature to a piece of data that is particular to the user to whom the data belongs as well as the data itself, certain types of fraud can be detected with respect to electronically-stored data.

Where It Occurs: Many types of data in a healthcare setting need to be associated with a particular individual who is responsible for that data. This applies to both stored and transmitted data. For example, a doctor who prescribes a chemotherapy regimen for a cancer patient should sign for that prescription; similarly, any subsequent message describing changes to that regimen made by an administering nurse should be signed by that nurse. Such a signature is also linked to data integrity, in making sure that data cannot subsequently be changed (either accidentally or intentionally) or denied. For instance, once a medical lab technician signs off on a report of test results for a patient, it should not be possible for someone else to change these test results or for that technician to deny that he did the associated tests.

Data authentication could be applied to all health-record systems as well as communications between all components of a computerized health care system (see Figure 1). Where available at present, data authentication is done by each health-record

[27] see footnote 6.

system individually, and given the need to protect the associated encryption and decryption keys, it seems unwise to separate this function from personal health information. That is, data signatures should be kept with the data.

What It Does: Data authentication technology is implemented using digital signatures. As originally described, a digital signature for a piece of data involves encrypting a digest of that data with the private encryption key of a particular user; as no-one else has that key, the signature can only be created by and is specific to that user. Hence, that user cannot subsequently deny that he made that signature. Moreover, as the digest used to create the signature is particular to the data, any attempt to change the data will result in a different digest, which can be recognized when the signature is decrypted. Within the limits of resolution of the method used to create the digest, the data cannot be altered once it is signed.

Note that a single digital signature on a message implies that the sender cannot deny sending that message; however, this does not prevent the receiver from denying that the message was received. This can be fixed with the addition of slightly more complex signature techniques.[28]

Limitations and Concerns: As data authentication is based on digital signatures which are in turn based on public-key cryptography, data authentication inherits all problems associated with these technologies. The resolution of the method used to create digests is also problematic. If the digest is so short that it describes a large number of very different pieces of data (as would be the case if the digest only counts the number of bits used to encode the data), then a careful intruder could modify the data without creating a digest different from that encrypted in the signature. However, more complex methods that yield more data-specific digests also necessarily create longer digests, whose encryption and storage overhead may make the use of signatures computationally too expensive. At present, there are few guidelines for striking appropriate tradeoffs between digest resolution and system efficiency.

[28] Kremer, S., Markowitch, O., and Zhou, J. (2002) "An intensive survey of fair non-repudiation protocols." *Computer Communications*, 25, 1606–1621.

2.2.7 Secure Remote Access [29, 30, 31, 32, 33]

Risks Addressed: Secure remote access prevents unauthorized users or systems from accessing or manipulating data while that data is being electronically exchanged between two systems. This is done by creating a secure channel for two-way communication between a pair of sites.

Where It Occurs: Many computer systems consist of a set of geographically distributed sites which communicate with each other over a network to perform tasks. Each such task is one site requesting a service of another site, where such services can be anything that a user typically asks a system to do. Additionally, many of the other security and privacy technologies, such as user authentication, trust management, and so on, can be distributed throughout the network or performed by a remote service by employing techniques of secure remote access. For example, a municipal health department server in Vancouver may automatically request epidemiological influenza data from a hospital in Winnipeg, a nurse waiting at an airport may use his laptop computer to request access to the files on his home office server over a wireless Internet connection, or a doctor sitting at the PC in her hospital office may order a particular set of tests for a patient of hers to be done at the lab downstairs. Although internet communication is most common, remote access can take place over a variety of network media, from dedicated telephone lines linking the organization to which both communicating systems belong to a public line owned by a third party to (in the case of wireless communication) radio waves in the air itself. As all media are open to eavesdropping and information exchanged in almost all healthcare tasks is private, it is crucial that these channels be augmented to be as secure as possible during remote access.

Secure remote access is a critical component of all software communicating in any secure network, including a healthcare system that most communicate over a network with other sites; this includes not only sites separated geographically but also sites operating within the same building, floor, or even room. Given the sensitivity of information, secure remote access must be provided by every site individually- it cannot provided as a data service.

---

[29] Strassberg, K. (2004) "Network Design Considerations In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) *Network Security: The Complete Reference*. McGraw-Hill / Osborne; New York. 193-212.

[30] Strassberg, K. (2004) "Network Device Security." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) *Network Security: The Complete Reference*. McGraw-Hill / Osborne; New York. 213-227.

[31] Strassberg, K. (2004) "Firewalls." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) *Network Security: The Complete Reference*. McGraw-Hill / Osborne; New York. 153–174. 229-245.

[32] Fortenberry, T. (2004) "Virtual Private Network Security." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) *Network Security: The Complete Reference*. McGraw-Hill / Osborne; New York. 247–262.

[33] Vladimirov, A. (2004) "Wireless Network Security." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) *Network Security: The Complete Reference*. McGraw-Hill / Osborne; New York. 263–294.

How It Works: Secure remote access technologies create reliably and robustly secure two-way communication channels between pairs of systems that wish to exchange information. Creation of such a channel requires that (1) the identities of each communicating system can be established by the other system, and (2) information can be exchanged simply and quickly without unauthorized access or interference between those systems. The former is essentially a system-level, two-way version of classical user authentication, and the latter involves not only making any hardware involved in the connection networks secure against eavesdropping but also ensuring that any data transmitted over the connection is securely encrypted using standard one- or two-key techniques as described in Section 2.2.5 . Using the strongest practical encryption schemes is particularly important in wireless communications, which are very easy to intercept.[34]

The required authentication and encryption technologies may be packaged together in the form of *Virtual Private Network (VPN)* software, such that two systems individually running the same VPN software package can easily initiate secure communication over public networks such as the Internet. As communication over such public networks typically involves transmitting messages over a route with several intermediate relay sites, VPN software can speed up transmission by determining and including full intermediate-site routing information in transmitted packets of data.

Limitations and Concerns: As secure remote access is based on both user authentication and data encryption technologies, secure remote access inherits all problems associated with these technologies. Perhaps the biggest problem in secure remote access is the opportunities it opens up for misuse; if so much as one of the systems on a group of systems communicating by remote access is breached, all systems will treat any communication from that system (whether it is authorized or not) as authorized. Thus, most attacks on remotely-communicating systems focus on the communicating systems themselves (especially small systems that are not as important and not as well protected) instead of the communication channels.[35] This can remedied indirectly by applying equal and rigorous levels of security to all communicating systems, regardless of size and importance, and directly by filtering both in-bound and out-bound communication traffic at each system to prevent propagation of unauthorized access in the event of a breach; the latter can be implemented in the VPN software package itself as a form of firewall.[36]

2.2.8 Trust Management [37]

Risks Addressed: In situations where users need to interact with systems for which they do not have explicit authorization, trust management makes sure that only users that are deemed trustworthy are granted access. In situations where data must be passed between

[34] see footnote 33.
[35] see footnote 29, page 203.
[36] see footnote 31.
[37] Li, H. and Singhal, M. (2007) "Trust Management in Distributed Systems." IEEE Computer,40(2), 45-53.

different systems, trust management may also be used to make sure that only data that can be trusted is accepted and integrated into a data store.

Where It Occurs: It is often the case that both patients and healthcare professionals travel outside the boundaries of home computer systems in which they are recognized and have certain rights and privileges. For example, a person whose family doctor is in Toronto may travel to, become sick in, and require local medical attention in South Africa; similarly, a doctor from Vancouver at a conference in Montreal may be called upon to help local physicians during an influenza outbreak. Traditional system-specific methods for granting authorization (see Section 2.2.2) may be difficult to modify in a timely fashion, especially if the medical situation is an emergency. Hence, there is a need for computerized healthcare systems to automatically and rapidly assess those other systems and system users that can be trusted and granted temporary authorization. This is most important in systems associated with primary healthcare; however, it would also be useful in medical research and administration (to make long-distance collaboration easier).

Similar situations also arise in data exchange between systems. For example, a healthcare system in Vancouver in the process of treating a tourist from Malaysia may have to decide whether disease antibody test results taken when the tourist was treated at a hospital in Fiji earlier that month can be integrated into the Vancouver hospital's EMR and used in the patient's treatment. In this case, trust is applied to the problem of data authentication, and trust management is useful in a similar range of systems as described above.

Trust management could be applied to health-record systems, applications, data services, and individual user computer systems that need to communicate. (see Figure 1). Trust management is arguably more valuable in the context of an EHR, which may have multiple systems communicating, than in an EMR tied to a close-knit community with social trust mechanisms. As establishing trust between systems is a complex process (see below), trust management is an ideal technology to subcontract to a data service.

What It Does: Trust management technologies essentially try to encode the processes by which human beings decide who they can trust and now much and in what ways they can trust them. In a situation in which a system A is trying to decide if it trusts a system B, A makes its decision based on information it accumulates about B. This information can be about abilities of or services offered by B (*credential-based trust*) or how B has behaved in previous interactions with other systems (*reputation-based trust*). This information is evaluated using a trust model, which outputs the types of trust that are appropriate. Judgments of trust between pairs of system can be chained together to allow systems that do not directly communicate with each other to trust each other. The goal of these technologies is ultimately to provide more flexible and general mechanisms for granting user authorization and data authentication.

Limitations and Concerns: While there are mechanisms available for secure exchange of credential and reputation information between systems, it is very difficult to create an adequate trust model to use this information when this information is true, let alone in

cases where an unknown part of that information is false. It has been equally difficult to find a general and reliable method for chaining pairwise judgments of trust together to establish indirect trust. Though a number of prototype trust management systems have been implemented over the last decade, these technologies are still in development and are not as ready for integration into a healthcare system as are more mature cryptographic, authentication, and authorization technologies described above.

2.2.9 Data Storage Management

Risks Addressed: Data storage management prevents unauthorized users from reading archived data and ensures that authorized users can read archived data.

Where It Occurs: Given the increasing amounts of data that is being generated within the healthcare system as well as the need to ensure access to this data for periods on the order of 50+ years, it is inevitable that certain data that is not in constant use will have to be archived. The data stored in these archives must be protected to the same degree as data stored in the main database system. Moreover, though the data in such archives must remain the same, it will have to migrate to new data storage hardware as technology advances. Both data archives and discarded data storage equipment provide opportunities for accidental loss or unauthorized access to data. For example, if decryption keys associated with encrypted archived data are lost, the data is effectively lost as well. Data may also be recovered from partially or incompletely erased memories of discarded data storage devices.

Data storage management is important for all health-record systems archiving data. (see Figure 1); Moreover, as all applications run on computer equipment and almost every such piece of equipment has local data storage which may retain traces of healthcare data, equipment-erasing technologies (see below) should be part of every installation.

What It Does: Data storage management technologies differ depending on whether they are dealing with data archives or discarded data storage equipment. In the case of data archives, if encryption is used, secure private decryption key archives must be maintained, and provisions made switch cryptographic technologies as cryptographic standards change.[38] Moreover, even though historical data archives are of secondary importance to current data storage, equal levels of protection with respect to user authorization and authentication, intrusion and malware detection, and data authentication should be maintained. In the case of obsolete data storage equipment, standard inventory systems should be used to record what has been done with that equipment, and appropriate technologies should be applied to ensure destruction of any stored data before the equipment is discarded or resold.

Limitations and Concerns: All problems associated with active data storage are compounded given the length of time that archives must be available; in particular, the probability of accidents due to even infrequent human error increases as the archives

[38] Buchmanns, J., May, A., and Vollmer, U. (2006) "Perspectives for Cryptographic Long-Term Security." *Communications of the ACM*, 49(9), 50–55.

ages. It has also been shown that current data erasing technologies vary wildly in their effectiveness, and short of physical destruction of the equipment, no method can guarantee that some forms of potentially useful data cannot be recovered from allegedly erased equipment.[39]

2.3 Privacy Technologies

2.3.1 User Identity Management [40, 41]

Risks Addressed: User Identity Management prevents any user of a system from acquiring identifying data of other users of that system. By allowing each user to specify and access systems using multiple (possibly partial) identities, the privacy of system users is preserved as much as possible.

Where It Occurs: Though computer systems have typically required users to specify all their identifying attributes at some point in order to obtain access to and make requests of systems, this does not mirror the way personal identity is used in everyday life. For example, while a patient requesting a medical consultation must disclose their full identity, a patient filling out a survey need only disclose certain general aspects of their identity (like age and gender), and a patient requesting a publicly-available pamphlet on hospital services need disclose no identifying aspects at all (except that she is a requester of information). In everyday life, a person has a collection of partial identities based on what needs to be known by others interacting with that person in particular situations, and the degree of disclosure in each identity is under the control of the person. This could also be true of how people interact with computer systems. In addition to controlling how much identifying information is disclosed in each system interaction, a user could also be able to query any system to find out how much identifying information the system has about that user.

User identity management could be used in all contexts in which user authentication appears - namely, all health-record systems, applications, data services, and individual user computer systems within a computerized health care system (see Figure 1). At present, user identity management is done either by individual users or, in the case of groups of closely-related applications, by a data service (see below). Given that identity management is complex, it may initially seem preferable to use data services for user identity management in all cases; however, this puts significant reliance on the quality of the data service itself.

What It Does: User identity management technology combines many of the aspects of consent and trust management - like consent management, individual preferences about

[39] Geiger, M. and Cranor, L.F. (2006) "Scrubbing Stubborn Data: An Evaluation of Counter-Forensic Privacy Tools." *IEEE Security & Privacy*, 4(5), 16–25.
[40] Claus, S. and Köhntopp, M. (2001) "Identity management and its support of multilateral security". *Computer Networks*, 37, 205–219.
[41] Damiani, E., De Capitiani di Vimercati, S., and Samarati, P. (2003) "Managing Multiple and Dependable Identities." *IEEE Internet Computing*, 7(6), 29–37.

identity expression must be gathered for particular system-interaction situations, and like trust management, negotiation must take place, in this case between what the user is willing to disclose and what the system requires to grant access. Identity management schemes range from the decentralized (in which individual users mange their identities either with [42] or without [43] the assistance of trusted third parties), to centralized, (in which a group of closely-related systems delegates identity-interactions with users to a single trusted third party as in ***Federated Identity Management (FIM)***.[44, 45] A number of prototype systems have been developed, many of which use public-key cryptography and PKI. The most mature of these prototypes operate within the FIM framework.

Limitations and Concerns: Given its basis in user-preference specification and interpretation and user-system negotiation, user identity management technology is necessarily complex. While the more mature FIM prototypes seem to function well and will fit in well with large healthcare organizations,[46] these prototypes have not yet demonstrated the full range of functionality required (in particular, the ability of a user to query a system about stored information on that user); moreover, their reliance on trusted third parties renders them susceptible to attacks on the certifying authority. Decentralized identity management schemes are preferable in this latter respect, but are unfortunately much less mature at this time.

2.3.2 Data Anonymization [47, 48, 49]

Risks Addressed: Data anonymization prevents any user from reading enough data to re-identify the individuals described in that data. By selectively modifying the data, the privacy of individuals described in the data is preserved. This is commonly considered a legitimate means of making that data available for secondary uses such as research or health surveillance purposes.

Where It Occurs: In a healthcare system, data about individuals must often be made available for research purposes. Ideally, each such release requires the consent of all individuals described in the data; however, this may be very difficult to do, given the number of individuals in the data as well as the number of possible research projects which may require that data. If individuals cannot be re-identified from released data,

---

[42] see footnote 40.

[43] Richardson, B.R. and Greer, J. (2004) "An Architecture for Identity Management." In *Proceedings of the Second Annual Conference on Privacy, Security, and Trust (PST'04).* 103–108.

[44] Shin, D., Ahn, G.-J., and Shenoy, P. (2004) "Ensuring Information Assurance in Federated Information Management." In *Proceedings of the IEEE International Conference on Performance,* Computing, and Communications. 821–826.

[45] Mead, B. and Wright, D.J. (2005) "Healthcare applications of federated identity management." International Journal of Electronic Business, 3(1), 88–105.

[46] See footnote 45.

[47] Chaytor, R. (2006) *Utility-Preserving k-Anonymity*. MSc Thesis / Technical Report #2006-01, Department of Computer Science, Memorial University of Newfoundland.

[48] Sweeney, L. (2001) *Computational Disclosure Control: A Primer on Data Privacy Protection*. PhD thesis, Massachusetts Institute of Technology.

[49] Willenborg, L. and deWaal, T. (2001) *Elements of Statistical Disclosure Control*. Lecture Notes in Statistics no. 155. Springer-Verlag; Berlin.

many would consider there to be no privacy risk to the individuals described in the data and no further reason to require consent for data release.[50]

Data anonymization will become important for any system components that release data for secondary use purposes (see Figure 1). At present, data anonymization is the responsibility of individual subsystems. Provision of this technology by a service provider would require particular caution, as it involves access to complete user identities.

It is also possible to use data anonymization for some kinds of primary care use, as a precaution in case of large scale data breaches. This is not generally considered a use of anonymization in the health care environment, however.

What It Does: Data anonymization technologies modify a dataset so that no individual person described in the data can be re-identified. There are a variety of such technologies differing in the types of modifications made to the data:

- **De-Identification**: Obviously identifying parts of the data such as names and addresses are removed. If names and addresses occur across several files in a data release and it would be useful to link the individuals described in the data across files, a related technique called ***pseudonymisation*** replaces the identifying parts of each record with a specially-created ID code and makes sure that records corresponding to the same individual in different files have the same ID code.
- **Perturbation**[51]: Potentially identifying portions of the data have their values changed randomly; this may also involve shuffling the corresponding attributes in different data records
- ***k*-Anonymization**[52, 53]: Data is modified by deleting or generalizing record values until each record is indistinguishable from at least *k-1* other records; this means that in the data release, each individual described in the data is now indistinguishable from at least *k-1* other individuals.

Limitations and Concerns: Despite the comforting claims implicit in the names of these various technologies, no method short of deleting or modifying all data in a dataset is guaranteed to prevent re-identification of at least some of the individuals described in a dataset. It must be realized that existing methods only guarantee degrees of, not total, anonymization.[54] There seems to be a tradeoff among the computational speed of an anonymization method, the degree of anonymity guaranteed in the data release, and the usefulness of that data release to researchers:

[50] This reasoning, while widely accepted, is subject to challenge, as indicated later in this report, in Part II in particular.
[51] See footnote 49.
[52] See footnote 47.
[53] See footnote 48.
[54] Ohno-Machado, L., Silveira, P.S.P., and Vinterbo, S. (2004) "Protecting patient privacy by quantifiable control of disclosures in disseminated databases." *International Journal of Medical Informatics*, 73, 599–606.

- De-identification and pseudonomyization are fast and resulting data releases are useful to researchers; however, they do not guarantee anonymity. It has been shown that given only gender, date of birth, and zip code, it is possible to re-identify more than 80% of the individuals in the USA[55]; subsequent work has shown that such re-identification is possible relative to other attributes, and it is impossible to guarantee which attributes can be re-identifying. Preliminary research from Ontario suggests that the disclosure might be statistically tuned to adjust the re-identification risks based on what public data is available.[56]
- Perturbation is fast and guarantees a fair level of anonymity; however, the resulting data releases are not useful for many important kinds of analyses, such as those that link particular attributes like age and gender to particular diseases.
- *k*-Anonymity guarantees a fair level of anonymity and can (in certain variants[57]) give data releases that are useful to researchers; however, it is computationally expensive for all but the very smallest dataset

Given this tradeoff, it is difficult to assess what method should be used in a particular situation, if any.

2.3.3 Privacy-Preserving Data Analysis [58]

Risks Addressed: Privacy-preserving data analysis prevents users performing certain types of queries which would provide enough information to re-identify individuals. By employing specialized techniques for combining and summarizing data spread over several datasets, the identity of individuals described in that data is protected simultaneously with making that data available for some types of data queries.

Where It Occurs: As mentioned above in Section 2.3.2 , in a healthcare system, information about individuals must often be made available for research purposes, and each such release requires the consent of all individuals described in this data. Data anonymization sidesteps this need for consent by modifying the data prior to release such that risk of identity disclosure for individuals described in that data is minimized. Privacy-preserving data analysis also sidesteps consent, this time by leaving the data unmodified and guaranteeing that no individual can re-identified by certain types of analysis as long as specified procedures are followed. These procedures assume that the data is scattered over several datasets and that this data is never accumulated in one place, let alone released.

Given the above, privacy-preserving data analysis is recommended for secondary use purposes (see Figure 1). As privacy-preserving data analysis is complex and operates over collections of datasets scattered over subsystems, it is an ideal technology to both subcontract to and implement as a data service.

---

[55] See footnote 48.
[56] El Emam, K., Jabbouri, S., Sams, S. Drouet, Y. and Power, M. (2006) "Evaluating common de-identification heuristics for personal health information", Journal of Medical Internet Research, 8(4).
[57] see footnote 47.
[58] Vaidya, J., Clifton, C.W., and Zhu, Y.M. (2004) *Privacy Preserving Data Mining*. Springer; New York.

What It Does: Privacy-preserving data analysis technology is a collection of versions of certain popular data analysis methods; as many of these methods are used within an area of Computer Science called data mining,[59] they are more popularly known as ***privacy-preserving data mining (PPDM)*** methods. Ordinarily, these methods operate on large single datasets and have all data (including identity) in full view to anyone performing the analysis. The privacy-preserving versions allow the datasets to be distributed, and guarantee that at no point can anyone performing the analysis have enough information to re-identify individuals described in the data. These versions are constructed using special mathematical techniques from a sub-area of cryptography called secure multi-party computation.

Privacy-preserving analyses available to date can determine the best ways to group data (*classification*), determine if and how certain quantities in the data are correlated (*regression analysis*), find rules describing what quantities are correlated in the data (*association rule derivation*), and detect unusual records in the data (*outlier detection*). Many of these have obvious applications in healthcare. For example, regression analysis can be used to establish the best chemotherapy treatments for particular types of cancers by looking at correlations among regimen type, cancer type, and patient survival, and association rule derivation could be applied to DNA sequence data from people with and without a particular genetic disease to find mutations correlated with the disease, which can in turn be used to create diagnostic tests and possibly treatments.

Limitations and Concerns: The specialized mathematics underlying privacy-preserving data analysis means that relatively few people can work with these methods. This has two problematic consequences. First, it is difficult to find people who can implement existing methods, let alone derive new ones. Second, it is not obvious precisely how the mathematical criteria of information disclosure risk implicit in these methods map onto real-world privacy concerns; moreover, these methods are only guaranteed to preserve privacy if certain procedures are followed, and it is often not clear what will happen if, either accidentally or maliciously, they are not followed. This provides many opportunities for misunderstandings about and exaggerated claims for these methods such as those that have hampered the widespread adoption of PKI technologies. For these reasons, there have been very few real-world applications of privacy-preserving data analysis to date. Hence, though offering great promise, such technologies are perhaps too immature for widespread applications in healthcare at this time.

[59] Hand, D., Mannila, H., and Smyth, P. (2001) *Principles of Data Mining*. The MIT Press.

2.3.4 Consent Management [60, 61]

Risks Addressed: Consent management prevents a system from manipulating data in a manner that is contrary to the stated preferences of the owner of that data. By encoding usage-preferences that can be automatically read and interpreted as necessary, people can prescribe the use of their data. This is often characterized as a form of individual control over the data.

Where It Occurs: Many activities in the healthcare setting require the consent of the patient; and new privacy laws require consent for different uses of personally identifying information. Consent in the context of a data record can be viewed as a specification of situations under which various data operations are permitted or denied. Patient consent (sometimes implied consent) is required in primary healthcare, so that a patient allows a doctor to collect, use and share their medical information or perform medical tests or surgical procedure. Consent is also required for secondary uses of patient data such as medical research. Consent management could be used to enforce these consent directives while records are being accessed.

Consent management could be incorporated into all health-record systems, applications, data services, and individual user computer systems within computerized health care systems (see Figure 1). At present, consent management has only been implemented separately in individual health-record systems. However, as interpreting electronically-stored consent directives, let alone reconciling consent permissions with conventional authorization permissions associated with users (see below) is probably going to be a complex process, consent management may be a good technology to use a separate data service. Consent will necessarily follow the data across multiple applications, so that a common service for consent is a logical approach. However, outsourcing the consent information does expose personal information to the service provider.

What It Does: Consent management technology is very closely related to user authorization technology - where user authorization specified data manipulation permissions relative to data users, consent management specifies such permissions relative to the individuals described by the data. Given this, it isn't surprising that attempts to implement consent management to date have either re-used existing user authorization technologies[62] or re-used the underlying philosophy of encoding permissions in data-objects.[63, 64] Of particular interest are e-consent objects,[65, 66] which

[60] Clarke, R. (2002) "e-Consent: A Critical Element of Trust in e-Business." In *Proceedings of the 15th Bled Electronic Commerce Conference*. Available online: http://www.anu.edu.au/people/Roger.Clarke/EC/eConsent.html

[61] Coiera, C. and Clarke, R. (2004) "e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment." *Journal of the American Medical Informatics Association*, 11(2), 129–140.

[62] Lee, G., Him, W., and Kim, D-k. (2004) "A Novel Method to Support User's Consent in Usage Control for Stable Trust in E-Business." In A. Laganaà *et al*. (eds.) *ICCSA 2004*. Lecture Notes in Computer Science no. 3045. Springer-Verlag; Berlin. 906–914.

[63] see footnote 60.

[64] see footnote 61.

are very similar to the authorization certificates used in PMIs (see Section 2.1.3). In current system proposals, an e-consent object is created and stored each time a data owner such as a medical patient issues consent, and this object is interpreted afterwards as necessary whenever that patient's data is manipulated. A consequence of this approach is that the consent information is tied closely to personal health information.

Limitations and Concerns: Pritts and Connor[67] review three Canadian projects (Alberta Netcare's Physician Office System Program, B.C.'s PharmaNet and Ontario's Drug Profile Viewer system) with respect to consent mechanisms. Technologies such as data masking, access permissions (via passwords) with appropriate over-rides and logging can be governed by and track individual consent in these systems, but without an integrated management system that automatically enforces consent policies or directives.

Outside a series of pilot R&D projects initiated by the Australian Commonwealth Department of Health and Aging,[68, 69] there are virtually no operational consent management systems that exercise such control and enforcement of consent. Though the demonstration systems appear to work well,[70] it is not known what problems may emerge when these systems are scaled up to work in practical healthcare settings and when full consent functionality is implemented. For example, problems may arise in reconciling consent-associated permissions specified by the data subject with possibly contradictory permissions generated by conventional user authorization procedures.

2.3.5 Privacy Rights Management[71]

Risks Addressed: Privacy rights management prevents a system from manipulating data in a manner that is contrary to the stated preferences of the system or person responsible for that. By encoding usage-policies that can be automatically read and interpreted as necessary, both systems and people are able to negotiate the use of their data.

Where It Occurs: Many activities in the healthcare setting require the sharing (either access and/or manipulation) of data between sites. For example, a consulting orthopedic surgeon may be called in to verify the cause of a swollen knee of a patient initially seen by a general practitioner, an epidemiologist may look for patterns of influenza outbreaks in the patient records of several regional hospitals, and a cancer clinic administrator may

---

[65] see footnote 60.
[66] see footnote 61.
[67] Pritts, J., and Connor, K (2007) The implementation of E-consent Mechanisms in Three Countries: Canada, England and the Netherlands, a report for the Substance Abuse and Mental Health Services Administration , U.S. Dept of Health. Online: www.ihcrp.georgetown.edu/pdfs/prittse-consent.ppdf
[68] Commonwealth Department of Health and Aging (2002) *Summary overview of the electronic consent R&D project*. Available online: http://www.health.gov.au/hsdd/primcare/it/sum_ overview.htm
[69] O'Keefe, C.M., Greenfield, P., and Goodchild, A. (2005) "A Decentralised Approach to Electronic Consent and Health information Access Control." *Journal of Research and Practice inInformation Technology*, 37(2), 161–178.
[70] see footnote 69.
[71] Korba, L. and Kenny, S. (2003) "Towards Meeting the Privacy Challenge: Adapting DRM." In *Digital Rights Management: Proceedings of the ACM CCS-9 Workshop (DRM 2002)*. Lecture Notes in Computer Science no. 2696. Springer; Berlin. 118–136.

ask for a quarterly report of the prescription-rates of all chemotherapy drugs dispensed to patients under the care of that clinic. Such data must frequently be obtained from others. Each data user should have a (preferably explicit) policy of how this obtained data is used and dealt with after use, e.g., whether it is subsequently retained and/or shared with other systems and, if so, how this is done. Knowledge of such policies is crucial, so that individual people and other systems can determine if they can share data with such a data user without violating their own privacy preferences or policies; if such violations occur, such knowledge is also a prerequisite to any subsequent negotiation between the data holder and data user about what portions of data (if any) can be shared.

Privacy rights management could apply whenever information is exchanged between entities operating under different policy rules or jurisdictions. Interpreting electronically-stored data usage policies, checking such policies against electronically-stored data-holder usage preferences (see Section 2.3.4) and negotiating about any violations that occur, will be a complex process, privacy rights management may be a good technology to be provided as a remote data service.

What It Does: Privacy rights management (PRM) technology allows data users to state their data-usage policies explicitly, thus enabling the matching of this policies to (and if necessary, negotiation of terms with) the data-usage preferences of data holders. As such, it requires policy expression, interpretation, and negotiation mechanisms. The first of these has been supplied by the ***Platform for Privacy Preferences Project (P3P)***[72] as a standard XML-based format for electronically encoding data-usage policies. Though interpretation and negotiation mechanisms were originally supposed to be part of the P3P standard, they were judged too complex to integrate, and have been left to individual software packages using P3P encodings. This could in theory be done by direct contact between users and holders, each of which is running the same interpretation / negotiation software package; however, the complexity of this task favours indirect contact between data holders and users via a trusted-third-party data service.[73]

Privacy rights management is very closely related to consent management – where consent management specifies the data-usage preferences of the data holders, privacy rights management expresses the data-usage policies of the data users. Given this close relationship, one would expect that the technologies implementing these two types of management would be developed in parallel and would integrate together well. However, this has not been the case. Privacy rights management (in particular, the P3P standard) seems to have been driven primarily by e-commerce companies and their need to increase consumer trust in (and hence use of) company websites[74, 75] This e-commerce context is even more obvious in the interpretation and negotiation mechanisms adopted within privacy rights management, which are derived from Digital Rights Management (DRM) technologies designed to protect the intellectual property of media companies.[76, 77]

[72] Platform for Privacy Preferences Project (P3P). Available online: http://www.wr.org/p3p/
[73] Linn, J. (2005) "Technology and Web User Data Privacy." *IEEE Security &Privacy*, 2(1), 52–58.
[74] Carnor, L.F. (2002) "Introduction to P3P." Available online: http://lorrie.cranor.org.
[75] see footnote 72.
[76] see footnote 71.

Historical development aside, the fact that privacy rights and consent management are closely related and solving similar problems suggests that, regardless of their historical origins, these technologies will develop in a closer fashion in future.

Limitations and Concerns: There are problems with privacy rights management technology at the level of both electronically-stored policy expression and interpretation. Though the P3P standard requires P3P policies to be consistent with the associated natural-language statements[78] of these policies, these two versions are not required to contain the same detail, with the natural-language version (by virtue of flexibility) frequently being more detailed than the P3P version.[79] Though a more flexible policy-formulation language than P3P would help, the consistency of stored and natural-language versions would still need enforcement. Furthermore, there is no guarantee that the policies are followed by the user that obtains the data. This can be remedied to a degree within a trust-management-like scheme by having trusted third party organizations that issue online privacy seals to policy-compliant organizations[80, 81]; however, this too is problematic: verifying compliance is error-prone and there are few mechanisms for disciplining a non-compliant organization aside from revoking the seal.[82]

3 The Evolution of Data Protection

Each of the technologies described in the previous section has some drawbacks, limitations and risks, and some of them are not mature enough for wide scale adoption at this time. Still, the review should give a general sense that the selection of security and privacy technologies described are quite powerful and should be more than adequate to support the privacy requirements of a computerized healthcare system. However, there is a great deal more involved than simply choosing a set of technologies and putting them in place. The kind of protection offered should be appropriate and adequate for its intended purposes accompanied by a clear and common understanding of what those purposes actually are (a theme that returns in parts II and III of this report).

For a technology perspective, there is a practical problem of fitting the technologies into an existing culture of health care information, existing procedures and protocols, and making all the different software and administrative systems and components work together. In the technology world, the related notion is that of system design or system architecture.[83]

There are developing standards which describe aspects of a computerized health care system, from general architectural and technology choices down to the detailed coding of

---

[77] see footnote 73.
[78] "Natural" language in this context means the policy would be written in a human language like English, rather than a language the computer can use to instruct a program.
[79] see footnote 74, Slide 7.
[80] see footnote 74.
[81] Greenstadt, R. and Smith, M.D. (2005) "Protecting Personal Information: Obstacles and Directions" *Fourth Workshop on the Economics of Information Security (WEIS'05).*
[82] see footnote 81.
[83] Sommerville, I. (2001) Software Engineering (6th Edition).Addison-Wesley; Reading,

individual health information transmissions. Since such standards are in various stages of general acceptance,[84] the critique that follows addresses issues without tracing the history or content of specific proposed standards. However, it is important to note that the discussion and development of these standards is an important way in which technology adoption progresses.

Rather than attempt an explanation of system architecting and design, this section examines some of the influences on the develop pment of the architecture of a computerized health care system *other than* availability of technology - influences arising from technology culture or political culture. These include historical trends in the development of computer systems (Section 3.1) some ideas or assumption arising from those trends (Section 3.2) that lead to common models of privacy and security (Section 3.3), a look at the Infoway project (Section 3.4) and some final observations regarding healthcare systems (Section 3.5).

3.1 Historical Characteristics of Computer Systems

The earliest computer systems appearing in the 1950s were developed for organizations such as businesses (notably banking) and government departments.[85] These were un-networked stand-alone systems, with a relatively small amount (by today's standards) of data which was specific to the organization owning that system. The evolution in complexity from these systems in the last 50 years has seen changes in three important areas: (1) The *amount of data* stored by an individual system has increased dramatically, from thousands to trillions of pieces of information; (2) a system is now typically composed of many *distributed* sites, some of which hold data and others which access and manipulate data. These sites communicate with each other and other systems over networks such as the Internet. (3) The *relationship of stored data to the hosting organization* has changed such that data has information about outside entities, which may is not necessarily "owned by" or "about" the entity hosting the data.

Two additional trends have also apparent generally and with respect to the specific technologies reviewed earlier: (1) *The Business Orientation of Technology Development*:[86] As many computer systems are associated with businesses and many computer-performed tasks (especially on the Internet) are commercial in nature, the majority of new computer technologies have been developed for (and are suited to) the needs of business organizations. With design methodologies and architectures developing to serve this marketplace, mature technologies and designs tend to be those related to classic business needs, in which the organization owns and maintains control

[84] Health Level 7 (HL7), an American National Standards Institute, for example, incorporates standards and templates for health information messages through a reference information model that is almost universal. Online at www.hl7.org. Other components of the HL7 model are not as widely adopted. In contrast, EHRCom (and associated standard CEN 13606) is a standard for communications between EHR systems developed in Europe which has raised some interest in North America, but is not generally adopted. ISO standard 18303 (International Standards Organization, online at www.iso.org) is a less referenced requirements standard for EHR architecture.

[85] Ceruzzi, P.E. (2003) A History of Modern Computing (Second Edition). The MIT Press.

[86] see footnote 85

over all of the data it hosts. (2) *The Vulnerability of Stored Personal Data*: As many organizations require personally-identifying information such as names, addresses, and established ID numbers to establish relationships with individual people, the ever-increasing amount and interconnection of such stored personally-identifying data are increasingly attractive targets for criminals interested in fraud, identity theft or those trading in this information.

3.2 The Rise of Security and Privacy

Security and privacy technologies tracked the development of and evolution of computing technology in the business world.[87] As the most basic need in early computer systems was to protect systems and stored data owned by the business, the first technologies to mature were simple security-related technologies, starting with user authentication and user authorization. As distributed systems came into existence, these were expanded to establish security in distributed systems composed of collections of computing-system sites. The sequence of this growth followed the needs of the businesses moving into a networked marketplace, including:

1. Facilitating communication between known network sites (implicating data encryption, secure remote access).
2. Protecting known sites from unauthorized access (data authentication, intrusion and malware detection, data storage management).
3. Facilitating communication with new sites outside the organization (including technologies in early stages of mature development, such as trust management).

More recently, privacy technologies have been under development. Initially, the focus was on protecting the privacy of users in large distributed systems (identity management). However, as ever-increasing amounts of personally-identifying information about individual people came to be stored, and with public attention to large scale breaches,[88] emphasis has turned to protecting the privacy of the individuals *described* in the stored data. This can be done automatically by modifying how the system operates on data (privacy-preserving data mining) or by modifying the data itself (data anonymization). Consent management represents an even more ambitious approach motivated as putting data protection under the control of the individuals described by the data, and allowing these individuals to specify the operations which can and cannot be performed on that data.

Two important conceptual tendencies can be seen arising out of these historical trends. The first may be termed the *Myth of Absolute Security*. The review of technologies illustrated that all of these technologies have weaknesses and can be circumvented by a sufficiently motivated, resourced and technologically astute adversary. Furthermore, complex systems are seldom implemented, maintained and administered perfectly or

[87] see footnote 106.

[88] Two incidents that received particularly widespread coverage in the mainstream media were the loss of tens of thousands of medical records from the Veterans Affairs in May 2006 and the theft of potentially millions of credit card transaction records from the TJX Companies Group in January 2007.

without mistakes or errors – no system can guarantee absolute security or privacy. Today's IT professionals understand that security and privacy is related to multiple aspects of organizational infrastructure and process, not just technology.[89] With media attention given to many prominent examples of data intrusion and breaches, absolute security isn't a widely held public belief either. Yet conceptual slips are often made that security solutions are a matter of correctly implemented computer technology, or that significant privacy or security problems would be solved with the "right" trust or consent technology, for example. Perhaps such slips are a hold-over from the days when computer systems created a natural security perimeter against intrusion by being isolated rather than networked, or a bias that computer solutions are less prone to corruption or failure than human solutions. Another probable explanation is that the organizational and administrative support for the technology is *assumed* to be in place and working. In any case, it is very easy to fall into the trap of thinking a certain technology in itself "solves" a security or privacy problem in some absolute sense.

The second conceptual tendency of note is a *Technological Bias Towards Security*. Security technologies are older, more mature and often form the basis or are a pre-requisite for establishing a privacy protecting technology. There are few technologies specifically designed to ensure privacy; moreover, only two of these (privacy-preserving data analysis and data anonymization) can continue to operate effectively if system security is compromised. Even these are essentially data protection schemes, as one would expect to evolve from the business-oriented tradition of the field. The result is a strong tendency to treat privacy technology as if it is necessarily an extension of security or data protection technology. In Part II of the report, this data protection orientation re-appears in the structure of legislation and policy rules. There are at least theoretically possible alternatives, such as a privacy system based on surveillance,[90] censorship[91] or private enforcement (akin to copyright protection). It is an open question whether such alternative are viable, but they do highlight the fact that technology has emphasized a particular privacy paradigm.

Whether these tendencies are artifacts of historical trends, business orientation of technology development, or the comparative youth of networking technology, they influence how privacy technologies are designed into existing systems. Some effects that seem to be logically related to these tendancies are:

> Aggregation of PHI records into *Breach Friendly Health Datasets (BFHD)*: using a common service or a single data store location means that a lot of information can be stolen in the event of an unauthorized access breach – it is a "breach-friendly" strategy. Leaving the data records distributed at individual clinic or hospital EMRs as separate sites on a network means each breach exposes less data. But economically and in terms of administration of technology, it is easier to create

[89] see footnote 106

[90] Dekker, M.A.C. And Etalle, S. (2006) Audit-Based Access Control for Electronic Health Records. Technical Report, EWI-DIES: Distributed and Embedded Systems, University of Twente.

[91] Qiu, J.L. (1999) "Virtual Censorship in China: Keeping the Gate Between the Cyperspaces." International Journal of Communications Law and Policy, 4. http://www.ijclp.org

fewer highly secure and private sites. Service providers also prefer a larger client base, which generally (although not necessarily) encourages more aggregated data. These highly secure service locations will then attract more customers, aggregating even more data, and making them even more attractive to the would-be intruder or data thief. This leads to improved security measures, which again makes the site appear a better place to store yet more health information. A cycle of increasing data aggregation may ensue.

Lack of remediation for breaches: If the BFHD is breached, auditing and logging technologies that can help locate the source of the breach, re-establish security, and correct the organizational or technological failure that produced the breach.[92] However, there are no technologies or designs directed to recovering data or minimizing the impact on a person's privacy following a breach – they are directed at preventing breaches or correcting infrastructure weaknesses. Individual remediation does not appear to be an objective of these technologies. As a related observation, there appears to be little or no interest in anonymizing information which is not intended for secondary use (i.e. in preparation for disclosure), which could reduce the impact of a breach.

Privacy-as-Security mindset: The bias towards interpreting privacy as a data security paradigm is suggested above, with the consequence that aspects of privacy are often recast in terms of security mechanisms. For one example, a common approach to consent management is to collect the subject's consent directives related to the various roles in the health care system (see various roles in Figure 1). By capturing what each role is allowed to do, the privacy technology of consent management can be built upon the security technology of role-based access control (RBAC). This is technologically clean, but limits consent to specific role based access directives.

3.3 The Security / Privacy Perimeter

System design and architecting plays an important part in development of software systems. Generally, the notion is that design follows a phase of identifying the needs and requirements of the system, and precedes activities of implementation and testing.[93] These phases generally have several iterations to reach a final product, and in large system, modifications and improvements continue throughout the life of the system.

In most cases, security and privacy requirements should be developed as part of needs and requirements gathering. This is particularly a concern when privacy and security are considered secondary issues, as the users and the developers concentrate first and foremost on the functionality of the product (Does it actually work? How will I get the lab reports?) It is becoming less common, although still a concern, that privacy and security matters are an afterthought rather than integrated into requirements phase of a

[92] Strassberg, K. (2004) "Incident Response and Forensic Analysis." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) Network Security: The Complete Reference. McGraw-Hill / Osborne; New York. 739-760.

[93] see footnote 83

system project.[94] Helping improve this situation are security and risk assessment tools with such designations as "Threat Risk Assessments" or "Privacy Impact Assessments", many of which are standardized through industry norms.[95]

At the point of choosing privacy and technology components for a system, it makes sense to use existing techniques and components that are proven and mature, and stay away from new experimental techniques. Thus, it is natural to turn to existing technologies, system concepts and general principles that are well accepted. This is simply good practice. However, it can also lead to superficial treatment of security and privacy with little analysis of the standard solutions. An ideal architecture plan would specify the security and privacy technologies that are part of a system, how these technologies interact among themselves and other components of the system, testing and maintenance stratagems, and, perhaps most importantly, the levels of security and privacy that will hold in the resulting system. Criticism is leveled that terms such as "security and privacy architecture" are used to create a façade of thorough deployment analysis, which upon examination amount to little more than selecting from a set of unrelated and weakly integrated security and/or privacy technologies.[96]

There are common conceptual frameworks (herein called *models*) that do appear to characterize the goals and structure of these architectures. Dominating all approaches is the ***Perimeter Model,***[97] where the objective can be thought of as building a wall around some system resources. Walls can be built around whole systems, such as a clinical EMR (a system perimeter) or around particular pieces of data, such as PHI (a data perimeter). Security technologies, such as user authentication and authorization, are thought of as who or what is allowed inside the system perimeter. In the case of more complicated technology like access control or consent management schemes, this can be thought of as a set of nested perimeter walls corresponding to increasingly more specific levels of protection. Clearly, this concept is oriented toward the privacy-as-security mindset.

Less influential is the *Surveillance Model* in which systems resources are protected by watching access of these resources and responding appropriately. This approach would rely partly on social engineering to discourage inappropriate access, as each user knows that they are being watched and can if necessary be dealt with in the case of an improper access. This would be difficult to develop under existing software methodologies that target software design goals, not social culture. To rely exclusively on a surveillance model would require (1) reliable logging, (2) clear access rules available to each user (3)

[94] Oppliger, R. (2007) "IT Security: In Search of the Holy Grail." Communications of the ACM, 50(2), 96-98

[95] For example, Standard IEC/ISO 17799 "Code of practice for information security management", International Organization for Standardization (2005)

[96] see footnote 94

[97] Rhodes-Ousley, M. (2004) "Risk Analysis and Defense Models." In Bragg, R., Rhodes-Ousley, M., and Strassberg, K. (eds.) (2004) Network Security: The Complete Reference. McGraw-Hill / Osborne; New York. 31-45. The single- and multi-layer versions of the perimeter model have been christened the Lollipop and Onion Models by Rhodes-Ousley.

an effective punishment mechanism for violators. The surveillance concept *is* reflected in logging, auditing and malware technologies that are used - however, this is really subscribing to the perimeter model: the objective is surveillance of the system perimeter and data perimeter, to detect breaches.

Communication between sites is an important aspect of modern EHRs, and therefore establishing security and privacy compliance lead to some kind of a *Negotiation Model*, facilitating co-operation among system components. Technologies such as trust and privacy rights management (P3P) reflect these requirements. One again, however, this is often framed in terms of a perimeter, as negotiation is conducted with sites *outside the perimeter* to establish whether they are allowed access. Terms such as the "circle of trust"[98] implicitly tie the perimeter notion to trust and consent.

Other influences on privacy and security system design are worth keeping in mind: many EMRs store part of their data in older "legacy" systems based on older technology which are difficult to incorporate into newer systems, or to integrate with newer technologies. This can discourage the serious consideration of some technologies which become too complicated to implement or preclude communication with legacy systems. This also encourages the perimeter model, as it is convenient to build a particular sort of perimeter around an existing legacy EMR, defining its rules and capabilities for interacting with newer technology.

Another important influence is legislative requirements regarding functionality, privacy protection, consent, and other elements in the health care system. This is substantially the concern of Part II of this report.

3.4 The Choices of Canada Health Infoway

Canada Health Infoway has an extremely difficult task. As a federally based entity with no jurisdiction over provincial health care, they have the job of encouraging harmonization of EMR and EHRs throughout the country to a level of interoperability that provides the capability to share (where appropriate) health information across the country. If the complexities of health care and technology in combination were not enough to deal with, they also have each province and territory with jurisdiction over its own health infrastructure. Technology adoption, legislation and policy infrastructure is moving at different speeds and in somewhat different directions on provincial and even regional bases. In this arena, there is no means to prescribe and dictate solutions. Instead, Infoway has supported the development of common design elements for EHR infrastructure, captured to a large degree in documentation as the *EHRs Blueprint*[99] and the accompanying *Privacy and Security Conceptual Architecture (PSA)*.[100]

[98] Mead, B., and Wright, D.J. (2005) "Healthcare applications of federated identity management." International Journal of Electronic Business, 3(1), 88-105.
[99] Canada Health Infoway *EHRS Blueprint – an interoperable EHR framework*, version 2, March 2006
[100] Canada Health Infoway *Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture*, version 1.1, June 2005

In developing a solution compatible with different rules and procedures, design choices, multiple EMR solutions with different solution vendors, different authority structure, and different levels of engagement for decision making, there is a significant challenge to produce something which is not entirely vague, general and targeted at the least common denominator.

Keys points of the architecture are the use of registries containing information to identify entities within the scope of the EHR, and a HIAL (Health Information Access Layer) to provide a common communication channel between different EMRs, applications and data services. The registries include a health care ***provider*** registry**,** a patient as ***client*** registry, and a ***user*** registry for EHR users. These registries do not have to house PHI themselves**,** but may contain non-health related information that can be used to identify and authenticate those that interact with (or are described in) the system. (Such information may be personal, without being specifically health-related). Separate EMRs or services can interrogate the registries to authenticate registration regarding access to or information in the EHR.

HIAL promotes interoperability partly by adopting the HL7 standard for messaging between sites and corresponding services. As long as different implementations of EMRs agree to adhere with a common set of messages defined within the HL7 standard, they will be able to communicate through HIAL. The effort to design these messages is active and ongoing.[101]

Infoway identifies many services that may be incorporated in an EHR. This list includes encryption, protocols (TCP/IP), routing, queueing, logging, and even an interoperability service[102]. These services may be combined (at the discretion of jurisdictions) into larger self-contained services that enable communication between EHR systems and their components. It is the role of a special service - the EHRS locator service,[103] operating between jurisdictional EHRs - to identify where particular EHR data (including PHI) is maintained. In principle, the data might be distributed among different EMRs or data storage locations distributed across the country.

The Privacy and Security Architecture document describes ten related services that may be incorporated into an EHR. These substantially reflect the security and privacy technologies discussed earlier, with the general implication that these services can be housed on sites independently of the PHI – possibly using private service providers at remote sites. Different EMRs may use any or all of the services, allowing communication between systems even if they do not have exactly the same capabilities.

The separation of different privacy and security capabilities into distinct services provides design flexibility, but leaves open the question of what the effects will be when these services interact. For example, multiple services, such as user authentication, identity management, identity protection and access control, all require some level of user

[101] The HL7 Canada group's website is st.infoway_inforoute.ca/content/hl7
[102] see footnote 99, page 140
[103] see footnote 99, page 187

identification. In other words, multiple services have to be independently trusted to properly construct and use identity information without being compromised. While the encouraged development of FIM approaches for the identity protection service[104] does alleviate the BFHD problem in the case of a breach, it is unclear how other identity-related services might be combined to benefit from this protection, or how these can be effective unless all entities using the EHR take advantage of the same services. There are three proposed models for access control services: (1) role-based, (2) work-group based and (3) discretionary access control, the latter encapsulating more complex descriptions of access permission. Here again it is unclear whether EMRs that adopt different models of consent will be able to share data.

The registry concept of separated data repositories is extended to support many of the services (domain repositories for clinical data, lab reports and prescriptions; shared repositories for clinical events and orders; longitudinal logging repositories). For example, an independent "consent directive"[105] repository is contemplated to support consent management. Independent like a registry, it would record consent decisions or directives issued by the individual or authorized substitute decision maker(s). In addition to providing the possibility of distinct or remote providers on a service-by-service basis, this flexibility allows the particular service to be upgraded if new technology becomes available. For example, simple consent mechanisms built upon RBAC could be upgraded if support for more sophisticated consent choices was developed. A significant issue for developing this technology, however, is whether consent directives made in terms of PHI can be separated from the PHI itself, which in turn raises the question of whether the consent directives also constitute or reveal information about the PHI.

It does appear to be the case that all these services must refer back to the registries to authenticate access to the EHR HIAL. Duplicate registries do not seem to be contemplated. In order for this to work, these unique registries *must* be trusted, which has crucial policy overtones. Either the registries are self-certifying, or some external (possibly statutory) authority will certify them. This begs the question of whether trust is meaningful if it cannot be withheld while still obtaining health care services.

Having an architecture designed around messaging and separate services has several advantages. It allows new technology to be developed incrementally, and added to the available services as they mature. It allows different EMR systems to interoperate even with a certain amount of different PHI capabilities. But even at this level of flexibility, the architecture becomes policy about what kinds of technology will develop.

As a counterpoint, consider an alternative design based on PHI data objects, in which each piece of PHI is accompanied by its associated access permissions, consent information, usage history and appropriate digital signatures. Under such a scheme, the only legitimately held PHI would have this information attached. It would not matter if the records were inside or outside a security perimeter, PHI could be tested for

[104] see footnote 100, page 77.
[105] see footnote 100, at page 120

inappropriate dealing in any context it appears. This suggestion is similar to the digital rights management (DRM) schemes developing in the area of copyright. No central certifying authority is required, and the data can be verified independently without consulting or trusting particular service providers or elements of a system. In fact, the data itself could be used to test the integrity of these system elements. This scheme has its own weaknesses, including data proliferation and particular vulnerabilities to data theft and forgery. However, consideration of such alternatives is not available with the technologies favoured by an architecture separating data and service components. This is an implicit policy choice about technology direction.

3.5 The Business of Healthcare Systems

The most mature technologies and design methodologies are fitted to the needs of the traditional business environment. The primary need of most businesses is security.[106] Businesses have well-defined user authorization; for example, their employees have well-defined system access responsibilities according to their roles in the business. Businesses can readily enact and enforce protections around aggregate data as required because they are generally in charge of controlling the data.

Some difficulties arise in businesses that stray from the classical business imperatives. Modern banking and e-commerce industries store personal data on individual customers, which imports privacy concerns. However, these difficulties have mitigating features - financial ID numbers and identities can be revoked and changed if disclosed, minimizing the consequences of system breaches, and as there a number of competing businesses to which a consumer can transfer their interactions if a particular business is problematic, providing economic pressure for such businesses to be as careful in matters of privacy as possible.

These features are somewhat different in healthcare systems:

- Healthcare systems have special implications for security and privacy: Unlike financial data and identities, no aspect of the health history of an individual can be revoked or changed if disclosed, and the consequences of disclosure are much greater for some individuals.

- Schemes developed in the business context may be a difficult fit in healthcare. For example, the doctor-patient relationship and interactions with other healthcare professionals is often fluid, and may be difficult to capture using a perimeter concept or schemes impose well-defined roles and responsibilities (such as RBAC). The relationship between federal, provincial, and regional health authorities is also complex, as is the relationship between hospitals, doctors, and patients. Analogies to standard business relations such as employees, agents, contractors, or clients has potential problems.

[106] Schweitzer, J.A. (1995) Protecting Business Information: A Manager's Guide. Butterworth-Heinemann; Newton, MA.

This does not mean that healthcare systems cannot be designed to have good security and privacy - rather, it means that care should be exercised when importing business solutions into healthcare:

- Attention should be paid (and to some extent, is paid) to research and development efforts focused on healthcare-oriented privacy-related technologies that are currently immature (consent management) or uninvestigated (privacy breach recovery)

- Alternatives to conventional (perimeter-oriented) security / privacy architectures should be considered, if only because it will serve to highlight conceptual biases in current technologies and architectures.

- Health information legislation and policy should take into account the current state of technology, not only to anticipate and deal with future legacy problems as new technologies mature, but also to ensure that policy is not overly influenced by cultural assumptions and biases accompanying the technology. This latter point is taken up in the next part of this report.

Part II: Legislation, Rules and Privacy Technology

1 Introduction

This part of the project examines the legislative and policy framework in which the privacy and security technologies for personal health information operate. The intent is to uncover potential problems in the interaction between these technologies and the relevant policies they should serve.

Section 2 ,

Privacy Rights & Regimes, follows the development of privacy rights in Canada, and Section 3 , *Canada's Data Protection Laws* explains the legislative framework and laws for data protection as they operate throughout Canada. These two sections represent a departure from the main thread of the report, since they engage specific health information technology issues in only a peripheral manner. They do, however, provide some legal context for the following sections.

Section 4 , *Health Sector Specific Personal Information Protection*, deals with health-information specific laws enacted in four Canadian provincial jurisdictions. It is in the context of this more specific legislation that the consequences and influences of technology is more clearly elaborated and discussed. It would be wrong to conclude that the connections between policy and technology are only applicable to those jurisdictions: it is simply easier to ground the observations in the more finely articulated legislation. Characterization of which particular observations apply to which Canadian jurisdictions outside of the four pieces of legislation is not something this report engages, but many of the concerns raised are ubiquitous.

The last two sections (5 and 6) follow the interpretation and application of legislation down into implementation and operational levels of organizations, by examining regulations and the use of policy impact assessments (PIAs) in the deployment of technology. On general legislative principles, legislation attempts to be policy-oriented and technology neutral, rather than prescribing operational choices and particular software choices. Dealing more closely with operational concerns, regulations and PIAs are expected to speak more directly to specific technologies.

2 Privacy Rights & Regimes

Internationally, privacy has historically been conceptualized as a right linked with notions of dignity and autonomy.[107] Canada signed on to this understanding of rights in 1976 when it acceded to the United Nations International Covenant on Civil and Political Rights, which speaks of privacy as a right in Article 17.[108]

[107] United Nations Universal Declaration of Human Rights Article 12. Available at http://www.un.org/Overview/rights.html.
[108] http://www.hrweb.org/legal/cpr.html. Canada acceded to this on 19 May 1976.

Domestically, Canada introduced provisions into the Canadian Human Rights Act in 1977[109] which covered information on natural persons that was held by the federal government and had been used in making decisions about the individual concerned. Although this Part of the Act is no longer in force, the decision to use the vehicle of the Canadian Human Rights Act is a significant one, underscoring notions of human dignity, which are inextricably tied to privacy.

Although the *Canadian Charter of Rights and Freedoms*[110]does not explicitly include privacy in its protections, some privacy interests have been found to be protected under section 7, 8 and 2(b) of the Charter.[111] Under the Charter, it is clearly established that privacy protection inures to persons rather than to goods or places.[112] This should not be taken to mean that privacy is of value only to individual persons or that privacy has no social value. As Justice Gonthier noted, privacy is integral to the "preservation of a free and democratic society."[113] Priscilla Regan conceptualizes this as privacy serving "common, public and collective purposes."[114]

While privacy was being recognized and protected as a right, however, concerns regarding how to operationalize privacy were moving in a different direction. Faced with information technology developments allowing public and private organizations to increasingly aggregate information about individuals, states began to govern such activities.[115]

As country-specific data protection laws were enacted, concern arose that disparate national data protection schemes could hinder the free flow of information across borders, causing disruptions in important sectors of the economy. Accordingly, both the Council of Europe[116] and the Organization for Economic and Cultural Development

---

[109] Part IV of the *Canadian Human Rights Act*, S.C. 1976-77, c. 33. Part IV of the *Canadian Human Rights Act* was repealed (S.C. 1980-81-82-83, c. 111 (Sch. IV, s. 3)) and replaced by the *Privacy Act* (S.C. 1980-81-82-83, c. 111, Sch. II).

[110] *Canadian Charter of Rights and Freedoms,* Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982.c. 11 [*Charter*].

[111] A.W. MacKay, "The Waves of Information Technology, the Ebbing of Privacy, and the Threat to Human Rights" (1999) 10:3 N.J.C.L. 411.

[112] *Hunter v. Southam*, [1984] 2 S.C.R. 145.

[113] *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773 at 789.

[114] Priscilla M. Regan, *Legislating Privacy: Technology, Social Value, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995) at 221 [Regan, "Legislating Privacy"].

[115] Roger Clarke, "Beyond the OECD Guidelines: Privacy Protection for the 21st Century" online: http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html#ScopeDP [Clarke] notes: "The first laws that expressly protected information privacy were passed in Europe in the early 1970s. The West German Land of Hesse passed its Datenschutzgesetz (Data Protection Act) in 1970, and that term quickly came to be used in virtually all discussions. Sweden's Data Act of 1973 was the first such legislation at national level. A succession of Continental countries followed, including Germany in 1977 and France in 1978."

[116] *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe Convention 108)* online: http://www.coe.int/treaty/EN/cadreprincipal.htm.

(OECD)[117] created documents that set out fair information principles and attempted to harmonize transborder data flow issues by setting standards of cooperation, consultation and assistance. These principles were expected to form a template for national legislation.[118] Seeking a binding, rather than guiding rules, in 1995 the European Union formally adopted the *Directive on the Protection of Personal Data With Regard to the Processing of Personal Data and the Free Movement of Such Data (EU 95/46)*.[119] The EU Directive was also predicated on fair information principles.

At their most basic, data protection instruments consist of a series of procedural directions which are intended to protect privacy by controlling the collection, use and disclosure of personal information. Thus, data protection appears to be concerned with procedures for privacy rather than with privacy itself. Indeed, Raab and Bennett concede that "privacy as a goal has often been transmuted into data protection."[120] However, the two are not synonymous. Data protection presumes the use and disclosure of personal information, thus creating (if anything) a limited right of control over what organizations do with one's personal information. There is little or no acknowledgement that one might wish to prevent anything being done with the information or prevent the information being collected in the first place. Instead, it focuses on reducing harm to the individual by limiting use or disclosure of the information.[121]

Although data protection schemes may be created in response to social issues or threats, the schemes themselves have an individual and transactional focus on personal data. This effectively isolates the analysis from the larger social value of privacy.

The review of privacy protection in Canada reveals an ongoing tension between two philosophical approaches – the recognition of privacy as a human right and the fair information principles model based on data protection. Over the past decades, there has been a conflation (in name if not in substance) of these streams. This is particularly dangerous – privacy entitlements have become limited to (and understood as) data protection entitlements and thus lessened in scope. At the same time, maintaining the language of "rights" around privacy creates a (possibly unwarranted) assumption that meaningful rights entitlements are protected.

3 Canada's Data Protection Laws

Canada's legislative framework for privacy is something of a patchwork. That is, rather than a few laws governing personal information, there are a multitude of relevant laws in

---

[117] *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* released 23 September 1980. Canada signed on June 1984. online: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[118] online: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html.

[119] Online: http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

[120] Charles D. Raab and Colin J. Bennett, "Taking the Measure of Privacy: Can Data Protection Be Evaluated?" (1996) 62 Int'l. Rev. Admin. Sci.535 at 537 [Raab and Bennett].

[121] *Ibid* at 540.

multiple jurisdictions. To provide a context for the legislation most relevant to data protection in health care, a review of the most relevant related legislation follows.

This review presents three different categories of legislation: public sector laws; private sector laws; and health-sector specific laws, which supersede other laws in some jurisdictions and are merely complementary in others. Public and private sector laws are discussed in this section. In the next section, health-sector specific laws are examined in terms of their policy orientation and relationship with privacy and security technology.

Each of these sections examine the rules for data protection, or what can be though of as the *data stewardship* responsibilities in terms of entities dealing with data. This is organized according to various activities regarding the data: collection, use, disclosure, secondary use, maintenance/retention, access (by the subject of the information), enforcement of rules, and breaches.

3.1 Public Sector Personal Information Protection

- Alberta: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F. 25 (hereafter "Alberta FIPPA")
- British Columbia: *Freedom of Information and Protection of Privacy Act R.S.B.C. 1996, c. 165* (hereafter "BC FIPPA")
- Federal: *Privacy Act*, R.S.C., c.P-21. (hereafter "Privacy Act")
- Manitoba: *The Freedom of Information and Protection of Privacy Act* C.C.S.M. c. F175 (hereafter "Manitoba FIPPA")
- New Brunswick: *Protection of Personal Information Act* S.N.B. 1998, c. P19.1 (hereafter "NB PPIA")
- Newfoundland and Labrador: *Access to Information and Protection of Privacy Act* S.N.L. 2002, can-1.1[122] (hereafter "NL/LB AIPPA")
- Northwest Territories: *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20 (hereafter "NWT AIPPA")
- Nova Scotia: *Freedom of Information and Protection of Privacy Act*, R.S.N.S. 1993, c. 5 (hereafter "NS FOIPOP")
- Nunavut: *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20, as duplicated for Nunavut by s. 29 of the *Nunavut Act*, S.C. 1993, c. 28, as am. (hereafter "Nunavut AIPPA")
- Ontario: *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F31 (hereafter "ON FIPPA")
- Ontario: *Municipal Freedom of Information and Protection of Privacy Act* R.S.O. 1990, c. M56 (hereafter "ON MFIPPA")
- Prince Edward Island: *Freedom of Information and Protection of Privacy Act* R.S.P.E.I. 1998, c. F-15.01 (hereafter "PEI FIPPA")
- Quebec: *An Act respecting Access to documents held by public bodies and the*

[122] It is Part IV of this Act that addresses the protection of privacy. Part IV has yet to be proclaimed in force. However, the Act has been reviewed and any deviation from the general principles is noted in this section.

Protection of personal information, R.S.Q. c. A-21 (hereafter "Quebec")
- Saskatchewan: *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01 (hereafter "SK FIPPA")
- Saskatchewan: *Local Authority Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. L-27.1 (hereafter "SK LAFIPPA")
- Yukon: *Access to Information and Protection of Privacy Act*, R.S.Y. 2002, c. 1 (hereafter "Yukon AIPPA")

General

All Canadian jurisdictions, federally, provincially and territorially, have public sector legislation that governs access to government and public body information. These Acts apply to information held by public bodies, such as health agencies, which are usually identified by the individual legislation. Some of the Acts explicitly reference or incorporate the fair information principles.[123] The Quebec Act s. 76-79 requires that anyone other than a natural person who is processing nominative information must notify the Commissioner (in the appropriate form) whenever a file is established or where the information provided in the original notification has changed.

These Acts deal with personal information of identifiable individuals, which is defined in the Act and is generally restricted to information in recorded form.[124] The Acts also deal with Public Information Banks[125] and set out offences and penalties.[126]

Only the British Columbia legislation explicitly requires a privacy impact assessment (PIA) to be conducted, although the Quebec requirement for notification of the Commission and receipt of approval is effectively equivalent. The federal government Treasury Board has instituted the *Privacy Impact Assessment Policy*, which applies to all government institutions listed in the Privacy Act schedule except the Bank of Canada. Similarly, the Saskatchewan government has adopted a privacy framework that imposes a set of obligations on government departments with respect to privacy and information management practices. This vehicle functions as a *de facto* PIA requirement.

Collection

Each Act (unless specified otherwise) requires that information be collected directly from the individual unless one of the enumerated exceptions applies. Obligations are set out to inform the individual of the purpose for collection, the authority for collection,[127] and to

[123] BC FIPPA Part 3, Manitoba FIPPA Part 3, NWT AIPPA Part 2; NS FOIPOP s. 24-31; Nunavut AIPPA Part 2; Ontario FIPPA Part 3, Ontario MFIPPA Part 2; PEI FIPPA Part2
[124] Alberta FIPA
[125] Alberta FIPA s. 87; BC FIPPA s. 69; Manitoba s. 75; NWT AIPPA s. 70; NS FOIPOP s. 48; Nunavut AIPPA s. 70; Yukon AIPPA s. 63; Ontario FIPPA s. 44-46; Ontario MFIPPA s. 34-35; Privacy Act s. 11.
[126] Alberta FIPA s. 92; BC FIPPA s. ??; NB PPIA Principle 6; NWT AIPPA s. 59; NS FOIPOP s. 47; Nunavut AIPPA s. 59; PEI FIPPA s. 75
[127] BC FIPPA s. 26

provide the name of an employee of the organization who can respond to questions about the collection.[128]

In Nova Scotia, unlike other public sector jurisdictions, the requirements for transparency with respect to the purpose of collection, the authority for collection, and the provision of contact information are found only in the provisions related to the directory of records. There is no specified obligation to inform individuals at the point of collection.

Maintenance/Retention

Once the information has been collected, obligations as to accuracy and retention are set out,[129] as are the rights of an individual regarding corrections to information and the correlative actions an organization must take upon receiving such a request.[130] New Brunswick's Principle 5 allows information to be retained by converting the information it into non-identifying form. Ontario's FIPPA s. 40 and MFIPPA s. 30 require that information that has been used by an organization be retained for the period prescribed in the regulations in order to ensure that the subject has a meaningful right of access.

Each Act contains some obligation to establish security against risks.[131] Ontario's FIPPA and MFIPPA spell out these obligations. Every head of an institution is required to ensure that reasonable measures to prevent unauthorized access to the records in her institution are defined, documented and put in place, taking into account the nature of the records to be protected. Every head is required to ensure that only those individuals who need a record for the performance of their duties shall have access to it. Every head is required to ensure that reasonable measures to protect the records in her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the record to be protected. In addition, FIPPA regulations contain specific provisions with respect to the destruction of information. In contrast, neither of Saskatchewan's public sector laws contains provisions for safeguarding the information, a fact that has been criticized by the Information and Privacy Commissioner.[132]

---

[128] Alberta FIPA s. 33, s. 34, BC FIPPA s. 27, Manitoba FIPPA s. 36, s. 37; NB PPIA Principle 2, Principle 4; NWT AIPPA s. 40-41; NS FOIPOP s. 24; Nunavut AIPPA s. 40-41; PEI FIPPA s. 31-32; Yukon AIPPA s. 29-30; Ontaro FIPPA s. 38-39; Ontario MFIPPA s. 28-29; Saskatchewan FIPPA s. 26; Saskatchewan LAFIPPA s. 24-25; Quebec s. 64-65; Privacy Act s. 4-5.

[129] Alberta FIPA s. 35, BC FIPPA s. 28, s. 31; Manitoba FIPPA s. 38; NB PPIA Principle 5, Principle 6; NWT AIPPA s. 44; NS FOIPOP s. 24; Nunavut AIPPA s. 44; PEI FIPPA s. 33; Yukon AIPPA s. 31; Saskatchewan FIPPA s. 27; Saskatchewan LAFIPPA s. 26; Quebec s. 72; Privacy Act s. 6.

[130] Alberta FIPA s. 36; BC FIPPA s. 29; Manitoba FIPPA s. 39; NB PPIA Principle 9; NWT AIPPA s. 45-46; NS FOIPOP s. 25; Nunavut AIPPA s. 45-46; PEI FIPPA s. 34; Yukon AIPPA s. 32; Ontario FIPPA s. 47(2); Ontario MFIPPA s. 36(2); Saskatchewan FIPPA s. 32; Saskatchewan LAFIPPA s. 31; Quebec s. 89-94; Privacy Act s. 12(2).

[131] Alberta FIPA s. 38; BC FIPPA s. 30; Manitoba FIPPA s. 41; NB PPIA Principle ??; NWT AIPPA s. 42; NS FOIPOP s. 24(2); Nunavut AIPPA s. 42; PEI FIPPA s. 35; Yukon AIPPA s. 33

[132] *Annual Report 2004-2005*, Office of the Information and Privacy Commissioner (Saskatchewan). Available at: http://www.oipc.sk.ca/annual_reports.htm. Pg. 14.

Access

Under the federal Privacy Act s. 28, notwithstanding the individual right of access to personal information, the head of the government institution may refuse access to information that relates to physical or mental health of the individual who requested it where the examination of the information would be contrary to the best interests of the individual.

Use & Disclosure

Use and disclosure of the information is restricted to the purposes for which it was collected or a use that is consistent with those purposes unless the individual has consented otherwise.[133] The requirements for such consent are set out in each piece of legislation. The Privacy Act s. 9 also requires that a record be kept of any uses or disclosures of personal information which are outside the purposes set out in the Index of personal information established under s. 11.

British Columbia makes a distinction between disclosures of information outside Canada and inside Canada. Section 30.1 requires a public body to ensure that personal information is stored only in Canada and accessed only in Canada unless the individual to whom the information pertains has consented to it being stored in or accessed from another jurisdiction or disclosure is allowed under the Act. Section 33.1 further provides that a disclosure outside of Canada can generally only occur if specifically consented to unless the minister responsible for the Act has by order allowed the disclosure.

Section 44(2) of the Manitoba Act speaks to the role of service providers. It requires that a public body that intends to transfer information to a provider of information technology services must enter into a contract with that provider for the protection of that personal information. It also touches on matters of data aggregation, providing for specific uses and disclosures that concern the linking or matching of information in different databases, a disclosure on a volume or bulk basis of personal information in a public registry, and another collection of information. Where such a request is directed to a department or government agency, this use or disclosure can only occur with the approval of the head of the public body and such approval can only be given once the advice of a review committee established under the Act has been received and considered.[134] Where the head is satisfied that the purpose cannot reasonably be accomplished unless identifying information is provided, obtaining consent would be impracticable or unreasonable, the use or disclosure is not likely to harm the individual(s), and the benefits to be derived are clearly in the public interest, approval may be given. The head of the public body must also approve conditions relating to the protection of the personal

[133] Alberta FIPA s. 39, s. 40; BC FIPPA s. 32, s. 33, Manitoba FIPPA s. 39, s. 40; NB PPIA Principle 5; NWT AIPPA s. 43, s. 48; NS FOIPOP s. 26-27; Nunavut AIPPA s. 43, s. 48; PEI FIPPA s. 36-37; Yukon AIPPA s. 35-36; Ontario FIPPA s. 41-43 Ontario MFIPPA s. 31-33; Saskatchewan FIPPA s. 28-29; Saskatchewan LAFIPPA s. 27-28; Quebec Public Sector s. 59, s. 67; Privacy Act s. 7-8.

[134] It is noteworthy that this does not necessarily seem to impose the obligation on health bodies to seek the input of review committees.

information, including security and confidentiality, removal and destruction of individual identifiers at the earliest opportunity, and any subsequent use or disclosure without the express written authorization of the public body, and requires that the recipient enter into an agreement to comply with the approved conditions.[135]

3.2 Private Sector Personal Information Protection

- Federal: *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5. (hereafter "PIPEDA")
- Alberta: *Personal Information Protection Act*, S.A. 2003, c.P-6.5. (hereafter "AB PIPA")
- British Columbia: *Personal Information Protection Act*, S.B.C. 203, c. 63 (hereafter "BC PIPA")
- Quebec: *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1. (hereafter "Quebec")

General

In most of Canada, the legislation governing the private sector is the Federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA applies except in provinces with legislation that has been declared substantially similar. To date, three provinces – Alberta, British Columbia and Quebec -- have enacted private sector privacy legislation that has been declared substantially similar.[136]

The federal, Alberta and British Columbia private-sector laws all share the same stated purpose: to govern the collection, use and disclosure of personal information by private sector organizations in a manner that recognizes both the right of the individual to have his or her personal information protected and the need of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate.[137]

PIPEDA incorporates the CSA Model Code Principles as Schedule 1 to the Act. The schedule should be read along with Sections 2-10 of PIPEDA to fully understand the legislative scheme set out therein. Of particular relevance are Sections 7 (setting out the circumstances when personal information may be collected, used or disclosed without individual consent); and Sections 8, 9 and 10 (right of personal access and challenge, format of information provided, and when access may be refused).

The two key notions of PIPEDA are "reasonableness" and "consent". For reasonableness, Section 5(3) of the Act specifically provides that personal information

[135] Manitoba FIPPA s. 46.
[136] Ontario's health-sector specific *Personal Health Information Protection Act* has also been declared substantially similar, however it does not cover all private sector activities in the province and thus will be discussed with the other sector-specific laws.
[137] PIPEDA s. 3; AB PIPA s. 3; BC PIPA s. 2.

only be collected, used and disclosed for purposes that a reasonable personal would consider appropriate in the circumstances. This standard is applied regardless of whether consent has been given for the collection, use or disclosure. As for consent, the general rule is that personal information can only be collected, used or disclosed with the knowledge and consent of the individual unless an exception applies or the information is excluded form the Act. [138]

The AB PIPA s.4(4) has a "grandfathering" provision that deems information collected prior to 1 January 2004 to have been collected with consent, while BC PIPA excludes from the purview of the Act information collected before the coming into force of the Act under s. 3(2)(i).

The knowledge requirement means that organizations must make a reasonable effort to ensure that the individual is advised about the purposes for which it collects, uses or discloses information. Purposes for the collection of information should be identified and specified at or before the time of collection.[139] If information is to be used for a new purpose, then a new consent is required unless the secondary purpose is required by law.[140]

Although PIPEDA generally does not apply to hospitals except to the extent that commercial activities are involved, it will apply to health care practitioners in private practice.[141] It used to be that all health information was excluded from Alberta PIPA, but after the coming into force in June 2005 of the *Personal Information Protection Amendment Act*, Section 4(3)(f) now excludes personal information as defined in the *Health Information Act*. – this means that health information that was collected by an organization for non-health care related purposes (for instance, employee information) may be covered by PIPA. Professional regulatory organizations are expressly included in the Act. The Act contains a special section that provides for the establishment of a professional code that must be consistent with the Act's provisions relating to collection, use and disclosure. A process has been established to authorize the regulatory authority to operate in accordance with the Code and to deem that "compliance with a term or condition imposed by the Minister or directed by the Commissioner" and thus in compliance with the Act. This authorization can be revoked. The Commissioner may also audit the personal information practices of an organization in order to ensure PIPEDA compliance.[142]

Unlike Alberta PIPA, health information falls under the rubric of BC PIPA. Also different from Alberta, regulatory bodies are covered under the public sector legislation, and therefore excluded from the application of the BC PIPA.

---

[138] PIPEDA Principle 4.3.
[139] PIPEDA Principle 4.2, 4.3.2; AB PIPA s. 11; BC PIPA s. 10.
[140] PIPEDA Principle 4.3.1.
[141] see the "PIPEDA Awareness Raising Tools" document at http://www.e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00207e.html.
[142] PIPEDA s. 18.

Collection

The purposes for which personal information is being collected must be identified during or prior to the collection. [143] Personal information may only be collected, used or disclosed by an organization with the knowledge and consent of the individual, unless specified exceptions set out in the legislation apply.[144] The collection of personal information must be limited to what is necessary for the identified purposes and should only be collected by fair and lawful means.[145]

Alberta has special provisions for the collection of personal information from a source other than the individual to whom the information pertains. If this is done with the consent of the individual, then the collecting organization must notify the disclosing organization that the individual has consented to the collection. If this is done without the consent of the individual then the collecting organization must provide the disclosing organization with sufficient information to allow the disclosing organization to make a determination as to whether the disclosure would be in accordance with the Act.[146] BC PIPA also has this latter clause.[147]

Use/Disclosure

Personal information should only be used and disclosed for the purposes for which it was collected, except with consent or as required by law.[148] It can be retained only as long as is necessary to fulfill those purposes. [149] AB PIPA s. 22 and BC PIPA s. 20 contain an exemption for disclosure of information without consent in the context of a business transaction (i.e. sale or transfer of business.)

Secondary Use

PIPEDA states that personal information may be used for statistical or scholarly study or research purposes where the criteria set out in the legislation are met.[150] BC PIPA has similar requirements.[151]

Alberta's PIPA allows an organization to disclose personal information without consent under a research agreement only the standards set out are met, including approval by a recognized research ethics review committee.[152]

---

[143] PIPEDA Principle 4.2.; AB PIPA s. 11; BC PIPA s. 10.
[144] PIPEDA s. 7; AB PIPA s. 7, s. 14; BC PPA s. 6, c. 12.
[145] PIPEDA Principle 4.4; AB PIPA s. 11; BC PIPA s. 11.
[146] AB PIPA s. 13.
[147] BC PIPA s. 10(2).
[148] PIPEDA s. 7; AB PIPA s. 16-17, s. 19-20; BC PIPA s. 14-15.
[149] PIPEDA Principle 4.5.2; AB PIPA s. 35; BC PIPA s. 35.
[150] PIPEDA s. 7(3)(f)
[151] BC PIPA s. 21.
[152] AB PIPA s. 20(q), Alberta Regulation 366/2003 (made under authority of AB PIPA s. 62(1)(q)).

Maintenance/Retention

These statutes require that organizations develop policies and procedures to enable them to execute their obligations under the Act, including the designation of a person responsible for the privacy program, and policies for the furtherance of the privacy program.[153]

Under these Acts, organizations are accountable for the protection of personal information under their control. Personal information must be as accurate, complete and up to date as is necessary.[154] It must be protected by adequate safeguards. Methods should include physical, organizational and technological measures, secure destruction and employee awareness and training about confidentiality and privacy.[155]

An organization must make available upon request information about their privacy policies and practices.[156]

Access

An individual has the right of access to her personal information[157] and has the right to seek correction.[158] Both these rights are subject to some limited exceptions as specified in each statute. Organizations must provide the means for an individual to challenge an organization's compliance with these principles.[159]

Disposal

BC PIPA allows for de-identification in lieu of disposal of information.[160] There are no other explicit rules for disposal, though as with public sector laws, disposal is usually referenced as part of the general "safeguards" obligation.

Enforcement

Individuals have the right to challenge compliance with the obligations of PIPEDA by filing a written complaint with the Office of the Privacy Commissioner.[161] The Commissioner has an ombudsman role, with the power to receive complaints, conduct investigations, publish findings and conduct audits and make recommendations.[162] In connection with complaints, the Commissioner attempts to resolve these through inquiry and mediation. The Commissioner publishes findings of an investigation and the

[153] PIPEDA Principle 4.8; AB PIPA s. 5-6; BC PIPA s. 4-5.
[154] PIPEDA Principle 4.6; BC PIPA s. 33.
[155] PIPEDA Principle 4.7; AB PIPA s. 34; BC PIPA s. 34.
[156] PIPEDA Principle 4.8; AB PIPA s. 6; BC PIPA s. 5.
[157] PIPEDA s. 8; AB PIPA s. 24; BC PIPA s. 23
[158] Principle 4.9, Principle 4.9.5, Principle 4.9.6; AB PIPA s. 25; BC PIPA s. 24.
[159] PIPEDA Principle 4.10; BC PIPA s. 5.
[160] BC PIPA s. 35(2).
[161] PIPEDA s. 11.
[162] PIPEDA s. 12.

Commissioner's recommendation.[163] A complainant may then apply to Federal Court[164] and the court may (among other things) order the organization to publish a notice of any action taken or proposed to be taken and award damages, including damages for any humiliation the complainant has suffered.[165]

The Alberta and BC Commissioners are not Ombudspersons, instead having the power to make orders that are binding. [166] The PIPA's also provide a civil remedy, which allows an individual to sue an organization (against which the Commissioner has made an order) and an individual (who has been convicted of an offence) for damages for loss or injury that have been suffered as a result of the breach of the Act.[167]

4 Health Sector Specific Personal Information Protection

In this section, the specific health-sector PHI legislation is examined for technology implications. The provisions discussed are generally illustrative of legislative tendencies, with jurisdictional differences noted, rather than commenting on the regimes of each province. Many of the overarching critiques are equally applicable to the general legislation previously discussed. Rather than repeat the same analyses for jurisdictions using similar principles but acting under more general legislation, the relevant connections with technology are noted in this section in the context of these more specific health-sector laws.

- Ontario: *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3. (hereafter "ON PHIPA")
- Alberta: *Health Information Act*, R.S.A. 2000, c. H-5 (hereafter "AB HIA")
- Manitoba: *Personal Health Information Act*, S.M. 1997, c. 51. (hereafter "MB PHIA")
- Saskatchewan: *Health Information Protection Act*, S.S. 1999, c. H-0.021 (hereafter "SK HIPA")

Currently, Manitoba, Alberta, Saskatchewan and Ontario have enacted health privacy laws. In the case of Ontario, this legislation has been declared substantially similar to PIPEDA and thus supersedes PIPEDA within that province. In the other provinces, the legislation operates concurrently with existing (and applicable) privacy legislation. In these cases, specific provisions in the health privacy laws may supersede, elaborate or modify provisions in the more general public/private sector legislation.

These laws apply to many bodies, including: regulated health care professionals; the relevant provincial health departments; certain health services, boards, authorities, councils or corporations; many health care facilities including hospitals; as well as other

[163] PIPEDA s. 13.
[164] PIPEDA s. 14
[165] PIPEDA s. 16.
[166] AB PIPA s. 52; BC PIPA s. 52.
[167] AB PIPA s. 60; BC PIPA s. 57.

entities or individuals as set out in their corresponding regulations. Each of these laws seeks to control the collection, use and disclosure of personal health information by specified health sector participants without impeding the delivery of health services.

General

These acts introduce the concept of a "custodian" or "trustee" of PHI,[168] who has the responsibility for the custody and control[169] of the patient's information. These custodians go well beyond the individual physician-patient sharing of information, giving custodial responsibility to the hospitals, health institutions, health agencies, and other government entities to protect and share records appropriately, store them in EMRs, EHRs, and govern the distribution of the information in terms of its collection, use and disclosure.

While this tacitly recognizes the increasing number of care-givers associated with a patient's interaction with health systems, it is not clear the distinctions intended in the notion of a custodian/trustee are effective. Looking at the roles of Figure 1 in Part I of this report, it seems apparent that health care providers need access to the PHI, but if the hospital is a custodian, who acts on its behalf to engage its data protection obligations? Administrators and privacy officers are candidates, as well as service providers and technicians.

One concept commonly voiced around custodial responsibility is the "circle of care", meant to encompass those directly involved with patient care delivery. [170] Although not a legislative term, from the review that follows, the legislation appears to distinguish custodial responsibilities from other roles in the computerized health care system along the lines of this notional "circle of care". However, the legislative mechanisms to distinguish custodianship, such as contracts, agency, implied consent,[171] and so on do not always find corresponding technology mechanisms. The security perimeter or ability to negotiate a "circle of trust"[172] in privacy technologies is not well characterized relative to the circle of care or custodianship in health care data management. If anything, trust management technology and access control allows the system to deal with those who are not implicitly trusted (such as remote EMRs or service providers) by applying technical mechanisms to mimic human trust mechanisms. If used as a surrogate for the circle of care, such technology arguably *expands* the circle whenever new parties are provided access to the information. As the rest of the review will demonstrate, this is not what the legislation intends.

---

[168] ON PHIPA s. 3; SK HIPA s. 2(t); MB PHIA s. 1(1); AB HIA s. 1(1)(f).

[169] The notion of "custody and control" is built into the definition of "health information custodian" in ON PHIPA s. 3 and "trustee" in SK HIPA s. 2(t). Although not built into the definitions, the AB HIA also uses the language of "custody and control" as for example in s. 7 and s. 8. MB PHIA is distinct in using the language of "maintenance" in s. 1(1) rather than custody or control.

[170] The term meets various acceptability, but it adopted in the "Pan-Canadian Health Information Privacy and Confidentiality Framework", Health Canada, December 31, 2004.

[171] see footnote 212

[172] see page 46

The definitions of "personal health information"[173] (PHI) are similar under each act. They include: information concerning an individual's physical and mental health identifiable by health information custodians/trustees; information concerning health services previously provided to an individual; and information obtained from an individual when they register or pay for health services, including health identification number, name, address, telephone number, billing information, eligibility information. Alberta,[174] Saskatchewan[175] and Ontario[176] deal explicitly with personal health information dealing with body parts or bodily substances or with the testing or examination of body parts or bodily substances.

Some of the Acts parse "personal health information" into discrete categories. "Registration information" is a subset of personal health information and in some cases may be treated differently.[177] Alberta also recognizes multiple categories of "individually identifying health information", "health services provider information" and "registration information",[178] permits the collection, use and disclosure of non-identifying health information for any purpose,[179] and stipulates that a custodian who intends to collect, use or disclose information should limit themselves to aggregate health information if that will meet the purposes, and if not, should proceed incrementally along the continuum of identifiability.[180] Saskatchewan specifically excludes statistical information and de-identified information from the purview of the Act[181] as does Manitoba.[182] Ontario's definition of personal health information is predicated on the information being "identifying".[183]

These categories of information may require identification in the EMR/EHR systems. Since the information is classified into these categories, if the consent management, auditing, and access control technologies are going to manage the different permissions, (such as registration information) these will have to be recorded. This raises the question of which of these rules can or will be imbedded in the technology for the EMR/EHR, and which must be enforced by other means. The recognition of registry-type data reflects the influence of the registry structure of the Infoway architecture.

With some distinctions, each Act recognizes the transfer of information to third parties for information management and processing,[184] putting in place regimes to govern these

[173] Or simply "health information" in the case of Alberta.
[174] Alberta HIA s. 1(1).
[175] Saskatchewan HIPA s. 2
[176] Ontario PHIPA s. 4.
[177] Saskatchewan HIPA s. 2, s. 28, Alberta HIA s. 36
[178] Alberta HIA s. 1(1).
[179] Alberta HIA s. 19
[180] Alberta HIA s. 57
[181] Saskatchewan HIPA s. 3(2).
[182] Manitoba PHIA s. 3.
[183] Ontario PHIPA s. 4
[184] Saskatchewan HIPA s. 18, Alberta HIA s. 1(1), s. 66, Manitoba PHIA s. 1. Ontario PHIPA s. 73 contemplates special provisions enacted by regulation concerning persons who provide goods or

transfers and to source responsibility in the organization itself rather than the third party processor or information manager. This essentially captures the role of the service provider and others that may not be custodians, or operating outside the immediate "circle of care". This can cause problems on several levels – when individuals fall into several roles, for example, depending on what actions they are performing in a particular case. While not impossible using user authentication, authorization and access control mechanisms, it does create a great deal of complexity for dealing with these different roles using fixed classifications. The worst scenario is having care providers "locked out" of accessing essential information. This is generally addressed by using over-rides, but one has to question the value of a secure perimeter model over a surveillance approach in the first place if over-rides are available.

Although consent requirements exist in these laws, each province deals with the issue differently. Saskatchewan and Ontario sets out the components of a valid consent and its operation (including withdrawal and limited time period validity)[185] Alberta specifically provides that the revocation of consent to disclosure must be provided in writing or electronically, must be signed and must meet the requirements set out in regulations.[186] Under these laws, consent is given for particular actions, not for the data itself. While this is part and parcel of the data protection approach embodied in the legislation, it is difficult to realize with a computerized system that operates on protection of data records rather than information privacy. This drives solutions towards more complex consent mechanisms tied to actions on data. Patients are provided with limited pre-selected forms of informational self-determination -- time-limited consents, withdrawal of consent and specific instructions about information. Current consent management technologies generally provide specific categories of consent, tied to disclosure directives which restrict access to specific roles. That is, the consent ends up based on RBAC[187] and any actual control is limited to specifying what category of worker is allowed to access which data.

Saskatchewan also recognizes the creation of a comprehensive health record for the purposes of the Saskatchewan Health Information System[188] and provides for the possibility of a specified written direction from the patient to prevent the disclosure of such a record to trustees.[189] Finally, Ontario has an interesting provision for the recognition of multiple facilities as one "custodian" with Ministerial order where all requirements are met.[190]

This is the only provision addressing the problem of multiple custodians. That is, if the service provider is providing record keeping for multiple custodians with multiple

---

services in order to enable a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information.

[185] Saskatchewan HIPA s. 6, 7, Ontario PHIPA s. 18, s. 19.

[186] Alberta HIA s. 34.

[187] see page 21

[188] Saskatchewan HIPA s. 2

[189] Saskatchewan HIPA s. 8

[190] Ontario PHIPA s. 3

conflicting internal policies and technologies, how can the technology comply with each one?

Collection

Data protection standards around data collection are fairly consistent throughout the statutes.

Purposes for which personal information is collected must be identified by the custodian/trustee at or before the time the information is collected. Each of the Acts has some form of this requirement – that the individual be informed of the purposes for which the information is being collected and of the contact information for someone who will be able to answer questions about the collection.[191] Alberta requires in addition that the individual be advised the legal authority for collection.[192] While Saskatchewan doesn't use "purpose" language, their requirement that trustees take reasonable steps on collection to ensure the individual is aware of her right to be informed about anticipated uses and disclosures[193] sets out a similar requirement. Manitoba does provide an exception for the requirement to notify of purposes, stipulating that notice of purposes need not be provided in a situation where the trustee has recently provided the individual with this information about the collection of the same or similar information for the same purpose or a related purpose.[194]

Nor is the mere identification of "a" purpose sufficient – rather, information may only be collected for legitimate purposes. Generally this is expressed as a lawful purpose that is connected with a function or activity of the trustee who is collecting it.[195] Saskatchewan parses the issue slightly differently, requiring that the primary purpose be something that can reasonably be expected to benefit the individual but also allowing for the possibility of a secondary purpose where it is consistent with some authorized disclosures.[196] In Alberta, non-identifying information may be collected for any purpose,[197] but the collection of identifying health information is valid only where authorized by law or if it relates directly and is necessary to enable the custodian to carry out an authorized use.[198]

There are also limits imposed on the amount of information collected, to only the information necessary for the stated purpose.[199] In Ontario this is further nuanced by the stipulation that personal health information should only be collected where other

[191] Manitoba PHIA s. 15(1)
[192] Alberta HIA s. 22(3).
[193] Saskatchewan HIPA s. 9.
[194] Manitoba PHIA s. 15(2).
[195] Manitoba PHIA s. 13(1), Ontario PHIPA s. 29
[196] Saskatchewan HIPA s. 24
[197] Alberta HIA s. 19. Note that in practice, there is no way of determining what attributes are "non-identifying" since it depends on external data sources. See Part I, Section 2.3.2 Data Anonymization''
[198] Alberta HIA s. 20.
[199] Manitoba PHIA s. 13(1), Ontario PHIPA s. 29.

information will not serve the purpose[200] and even then, collection must be limited to that reasonably necessary to meet the purposes.[201]

Each of the Acts provides that information should be collected directly from the individual unless one of the specified exceptions applies.[202] Although the Acts do not speak explicitly of collection with consent, it seems intuitive that collection directly from the individual would be collection with consent as long as the requirements about notice and transparency are met. Ontario also contemplates the collection of health information directly from an individual, who is incapable of consent, but only where the collection is reasonably necessary for the provision of health care and it is not reasonably possible to obtain timely consent.[203]

When collecting information, the trustee should take reasonable steps to ensure the information is accurate and complete.[204] This is especially the case where collection is from a source other than the individual.[205]

Alberta explicitly contemplates the situation where information is collected by an affiliate of the custodian rather than by the custodian herself, and specifies that this may only be done in accordance with the affiliate's duties to the custodian.[206] Although technically this creates a gap between the custodian herself and the collection, the effect should be the same as had the custodian collected the information herself.

Alberta also provides for a situation where information is collected using a device that may not be obvious to the individual (such as a camera, recording device etc.) and requires written consent for such collections be obtained in advance of the collection.[207]

Information collection (except in Alberta, which recognizes the potential of information captured through invisible electronic means) happens at the point of patient contact with the system. Privacy rights dictate that that these conditions be demonstrably and verifiably met. This is again a case in which the technological burden, if technology is implicated as a compliance solution, is significant.

The information needed includes: the purposes of collection, legitimate purposes for collection (from the legislation) characterization of "necessary for the stated purpose", affiliate and custodian obligations, and possibly the means of collection. It is then open to question whether there would be a perimeter protection solution (akin to user authentication or consent management) or whether the system would simply log and audit these factors. The logical implication is that there is little, if any, belief that these legislative requirements will be enforced by technological means. Certainly the

[200] Ontario PHIPA s. 30(1)
[201] Ontario PHIPA s. 30(2)
[202] Manitoba PHIA s. 14, Saskatchewan HIPA s. 25, Alberta HIA s. 22, Ontario s. 36(1).
[203] Ontario PHIPA s. 36(2).
[204] Saskatchewan HIPA s. 19
[205] Saskatchewan HIPA s. 25(3).
[206] Alberta HIA s. 24
[207] Alberta HIA s. 23

mechanisms discussed in Part I do not contemplate any enforcement of collection restrictions, as consent management and trust management are directed toward access and disclosure. There are experimental approaches to technology directed to the collection and enforcement of such information,[208] but these are far from mature or widely adopted.

Use

Under the data protection models, knowledge and consent of the individual are required for use of the information; and information shall not be used for purposes other than those for which it was collected except with consent or as required by law. These Acts are consistent with that requirement, generally stating that health information may only be used with consent unless one of the listed exemptions applies. The existence and extent of such exemptions looks towards the institutional needs and business imperatives of health privacy protection.[209] From this perspective, the rules are about removing liability for acts done without consent. If the data stewardship was not the dominant paradigm, the legislation might look toward the effect of these provisions on privacy rights.

The recognized exemptions are fairly standard – provision of health care, prescribed purposes under the act, a purpose that will benefit the individual. However, different jurisdictions contemplate different allowable uses. Saskatchewan, for instance, sees the process of de-identifying information as an acceptable use.[210] Other jurisdictions recognize internal and systemic management and planning as acceptable uses.[211]

This also points up once again the limitations of the consent model[212] given that patient consent or lack thereof may be trumped by legislated exemptions. Informational self-determination is weakened by the existence of rules for information flow that circumvent consent and privacy. While this is expected in seeking a balance between privacy and data sharing requisite in health care, the relationship between planning and management and the technology chosen is not recognized. That is, the technology itself may trigger many of the exceptions.

---

[208] Hermaneutic approaches show some promise of being able to compare the semantics of data activity, but this is very experimental work. E.g. "Applied hermeneutics and qualitative safety data", Brendan, W., Ross, A. & Davies, J., *Human Relations* 2003, 56(5) pp. 587-607

[209] see Part I, Section 3.5 The Business of Healthcare Systems

[210] Saskatchewan PHIA s. 26

[211] Alberta HIA s. 27.

[212] The vocabulary around consent is somewhat problematic. Strictly construed, *implied* consent would refer to consent implied by the actions of the individual, distinct from statutory *exceptions* to consent requirements. But "implied" is commonly understood as an antonym for "explicit", covering both consent by implication and statutory exceptions. Unless context indicates otherwise, this latter conventional meaning of "implied consent" is used in this document. To make things further confusing, some regulations or statutes describe contexts of implied consent as well as listing exceptions to consent requirements. "Consent model" is used here to capture the entire milieu of explicit, implied and statutory consent as interpreted by privacy and health care practitioners.

Differences between provincial law with respect to consent requirements have been captured elsewhere using additional terms such as "no-consent" and "deemed consent", for example *Pritts & Connor* (see footnote 67) and *Infoway EHRi P & S* (see footnote 100 at p. 28)

Where information is used, it may only be used for the purposes for which it was collected unless the specified exemptions are met.[213] Further, only such information as is necessary to meet the purpose should be used[214] and only those employees or agents who need to know information in order to fulfill the purpose should have access to it.[215]

Where a trustee is also an employer, health information of an employee or prospective employee cannot be used without consent for an employment purpose.[216] Where use of the information is authorized, the information may be provided to an agent to use for that purpose on behalf of the custodian.[217] Alberta explicitly prevents affiliates of a custodian from using health information in a manner not in accordance with their duties to the custodian.[218]

The comments regarding relevant technological solutions made under the Collection section also apply here. Consent management based on RBAC is insufficient for this mix of complex and varied consent regimes, as they are suited to deal with access control almost exclusively. Surveillance/logging may play a role in recording use, or reasons for use (some systems provide this), and categories for these elements can be developed under HL7, for example. But validation or enforcement of such "usage" entries is not contemplated, probably because of administrative and labour implications or expectations they may create. Even logging usage activity without validation may create onerous overhead, although the ongoing requirements of transparency and openness might suggest that information use should result in the logging of when information is used, what information is used, what purposes it is used for and the authority for that use.

Ontario regulates the use of information that was collected or "created"[219] which adds an important nuance, since logging and other computer activities logically "create" information. In a similar vein, Alberta recognizes the possibility of information having been collected but not recorded or stored, and stipulates that this information may only be used for the purpose for which it was provided to the custodian.[220]

This reveals the disconnect between information and records. The legislation and technology both fail to recognize the importance of information until it is reduced to records. This may stem from the history and dominance of the perimeter model and associated mechanisms, so that there no other modes of understanding privacy protection as rights, surveillance or other alternatives. The laws are grounded in a "custody and control" model that is predicated on the notion of "records" rather than "information" itself.

[213] Manitoba HIA s. 21, Ontario PHIPA s. 37(1)(a)
[214] Manitoba HIA s. 20(2)
[215] Manitoba HIA s. 20(3).
[216] Saskatchewan PHIA s. 26(3).
[217] Ontario PHIPA s. 36(2).
[218] Alberta HIA s. 28
[219] Ontario PHIPA s. 37(1)(a)
[220] Alberta HIA s. 29.

Disclosure

Data protection rules state that information must not be disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Information should be limited to the minimum necessary to accomplish the purpose.[221] Disclosure to employees and agents should also be limited to that necessary to accomplish the purpose.[222]

Health information may only be disclosed with consent unless the specified exceptions are met.[223] The criteria for "consent" in such cases are set out in Alberta's legislation.[224] Affiliates or employees of the custodian are bound not to disclose information in any manner not in accordance with the affiliate's duties to the custodian.[225] Manitoba has similar requirements for its information managers.[226] Ontario's law explicitly notes that a permissive disclosure provision in the Act does not constitute a duty to disclose, nor does the ability to disclose without consent prevent the custodian from seeking consent before disclosure.[227]

This also raises the question of whether these exceptions, which replace patient control, are to be logged or enforced by the technology, and the limited expectation that existing technologies will monitor or validate this activity. In the case of such permissive scenarios, logging could also be implicated in order to record the factors motivating the custodian's choice to exercise her discretion.

The notion of extended disclosure within the "circle of care" is reflected in each of the Acts. In Alberta, for purposes of treatment, information may be disclosed without consent to another custodian for any or all purposes for which use is authorized[228] or to a person responsible for providing continuing treatment and care to the individual.[229] Manitoba allows this unless the individual has instructed the trustee not to make such a disclosure and then must still be limited to only that information necessary for the purposes.[230] Ontario, on the other hand, allows for this only where it is not possible to obtain consent in a timely manner and the individual has not expressly instructed not to disclose.[231] Rather than permitting disclosures without consent for these purposes, Saskatchewan deems there to be consent for a disclosure for the purpose for which information was collected or a consistent purpose or a service which has been requested or is required.[232] Such disclosures are authorized only where they are in accordance with

[221] Manitoba PHIA s. 20(2), Ontario PHIPA s. 30(2), Saskatchewan s. 23(1).
[222] Manitoba PHIA s. 20(3) , Saskatchewan s. 22(2)
[223] Ontario PHIPA s. 29, Saskatchewan HIPA s. 27(1).
[224] Alberta HIA s. 34.
[225] Alberta HIA s. 43
[226] Manitoba PHIA s. 25
[227] Ontario PHIPA s. 6(3).
[228] Albeta HIA s. 35(1)(a)
[229] Alberta HIA s. 35(1)(b)
[230] Manitoba PHIA s. 22(2)(a), s. 22(3)
[231] Ontario PHIPA s. 38(1).
[232] Saskatchewan HIPA s. 27(2)

ethical practices of the profession or where acceptable policies and procedures are in place to restrict use or disclosure of the information to that for which it was disclosed.[233]

Saskatchewan explicitly provides that information disclosed in this way to another trustee becomes part of both records.[234] Where the information is disclosed to a non-trustee, the discloser must verify the identity of the recipient and take reasonable steps to ensure that person is aware that information may not be used for any purpose other than that for which it was disclosed.[235]

Ontario permits some limited disclosures of information for specified purposes in the cases of health facilities[236] and identification of deceased.[237]

Finally, exceptions for disclosure for a variety of systemic purposes are included in the Acts, including: to a health professional body (with agreement as to confidentiality)[238]; for justice system purposes[239]; health system purposes (after preparation and submission of a PIA to the Alberta Privacy Commissioner)[240]; and public policy purposes.[241] Ontario too recognizes a variety of health systems purposes as legitimate disclosures[242] and Saskatchewan allows disclosure without consent for the provision of health and social services where it is clearly of benefit to the individual and not reasonably practicable to obtain consent.[243]

The circle of care notion has already been noted as a difficult one to implement in technology terms. As patient autonomy is trumped by the needs of the health care delivery and the nominal exercise of physician or custodial discretion, the "circle" may expand to the point where everyone except the patient may conceivably end up within the circle of care. Once the data is shared with service providers, administrators, and others it has very little recourse in terms of effective custodianship. Trust technologies, authentication, PKI and other techniques will either provide access or not – it is difficult to see how some entities that gain access are not within the "circle" regardless of legislative nuances. The service provider, for example, has greater expertise and competence in handling, protecting or stealing the data than the physician, pharmacist or other custodian – it is difficult to see how they are not inculpated into the "circle of care". Technologically this is consistent with the "perimeter model", but has the effect of exponentially increasing the existing risks of such a model.

---

[233] Saskatchewan HIPA s. 27(3)
[234] Saskatchewan HIPA s. 0
[235] Saskatchewan HIPA s. 21.
[236] Ontario PHIPA s. 38(3)
[237] Ontario PHIPA s. 38(4).
[238] Alberta HIA s. 35(4)
[239] Alberta HIA s. 37.1, 37.2, 37.3,
[240] Alberta HIA s. 46(1)(b)
[241] Alberta HIA s. 39-40.
[242] Ontario PHIPA s. 40 – 46.
[243] Saskatchewan HIPA s. 27(4)(j). In such cases, s. 27(6) restricts what can be done with the information.

Technological responses that can further delineate access capabilities and controls within the EHR or EMR are available – federated identity management, for example, can provide some restrictions to identity control within different components in the system, limiting exposure of the data. However, it is not the custodians who end up managing or controlling these techniques or technologies.

The lack of autonomy can be more clearly demonstrated by the inability to recapture PHI from the system. Once entered, the data can not be effectively withdrawn, since withdrawal is not retroactive in legislation. The question then arises, what happens if the patient no longer trusts or looses trust in the system? Under role-based consent directives, no patient can exclude particular service providers, for example, even if they have a serious breach and the patient wants their information out of their untrusted hands. In the computerized health systems contemplated, most Canadian have one care facility available, which means they have one set of EMRs and service providers. If they do not trust those technologies or services, there is no practical alternative. If you cannot withdraw trust, or it is statutorily or technologically mandated, the concepts of trusted third parties and trust management imbedded in the technology become little more than a façade. This differs dramatically from the business and networked environments where these security technologies matured: you can bring your financial data to another bank, remove a web site from a list of trusted sites, or seek an alternate certification authority. The lack of alternatives means there is no economic or business incentive to act in a trustworthy manner – the consumer must rely on oversight and enforcement mechanisms, and hope the technologies are responsive to those influences.

In Alberta, disclosure of information without consent under one of the specified exceptions requires a note to be made of who the disclosure was made to, the date and purpose of the disclosure, and a description of the information disclosed. However, where the information is contained in a computer database which automatically creates an audit trail including the user ID of the custodian who accessed the information, the date and time of access, and a description of the information this note is unnecessary. In either case, the audit information must be retained for 10 years following the date of disclosure.[244] This requirement is, at least to some degree, quite clearly motivated by an understanding of technological capacity as it imports the knowledge and function of audit trail technology. The effect, however, whether of a "note" or of audit trail information, is again an increase in logging and a correspondingly larger (and hence greater privacy risk) record.

In Alberta, some disclosures require the custodian to inform the recipient in writing of the purpose and authority under which the disclosure is made.[245] Saskatchewan requires that the individual be informed of all disclosures made without consent.[246]

[244] Alberta HIA s. 41, Ontario PHIPA s. 39
[245] Alberta HIA s. 42.
[246] Saskatchewan HIPA s. 10

Alberta recognizes the possibility of information having been collected but not recorded or stored, and stipulates that this information may only be disclosed for the purpose for which it was provided to the custodian.[247]

Ontario recognizes the possibility of situations where the custodian is prevented by express patient instructions from disclosing some or all information which the custodian believes is reasonably necessary for the provision of health care. In such situations, the custodian is permitted to notify the person to whom information is disclosed of this fact.[248] Again patient autonomy is superseded by the needs of the health care system and the need to avoid liability.

In general, the technologies for consent management based on authorization (principally of the RBAC type) support the tracking, logging, and enforcement of disclosure requirement, since it ties consent to access. Little modification to this type of technology would be needed to also record the statutory exceptions which apply to other disclosures, or the purposes for which those disclosures are made. Whether this information can be practically captured (who would enter the data?) is a separate concern.

Of course, not all information is covered by these Acts. In some jurisdictions, the Act does not apply to information that is not individually identifying.[249] Somewhat similarly, Alberta allows non-identifying health information to be disclosed for any purpose.[250] Where the disclosure is to a non-custodian, the person must be informed of their obligation to notify the Alberta Privacy Commissioner of any intention to data-match before proceeding with data-matching.[251] Although Ontario does not have such a requirement explicitly, it does provide that personal health information should not be disclosed if other information would serve the purpose.[252] Saskatchewan too requires that where practicable, trustees must disclose only de-identified information unless it will not be sufficient to meet the purpose.[253]

The notion that de-identified information has no privacy issues is problematic. Anonymization technologies and measures are not mature, and the fact that increased aggregation of data makes the data more susceptible to re-identification should raise concerns around such provisions. The fact is that one cannot reliably predict on the basis of characteristics of the record itself (without context of its disclosure), how identifying it might be.[254]

[247] Alberta HIA s. 44
[248] Ontario PHIPA s. 38(2).
[249] Manitoba PHIA s. 3, Saskatchewan HIPA 3(2)
[250] Alberta HIA s. 32(1).
[251] Alberta HIA s. 32(2)
[252] Ontario PHIPA s. 30(1)
[253] Saskatchewan HIPA s. 22(4).
[254] see Part I, Section 2.3.2 Data Anonymization ''

Secondary Use

Most of the Acts include provisions for whether (and how) information may be used in research, and some also recognize other systemic uses.

In Saskatchewan, information may be used or disclosed for research purposes with express consent where specified criteria have been met, including an assessment that the project is not contrary to public policy; project approval has been received from a Research Ethics Committee, an agreement is in place to restrict further use or disclosure of the information and to provide appropriate security and confidentiality; and arrangements have been made specifying return of the data and/or destruction.[255] Where it is not reasonably practicable to get consent, information may be used or disclosed for research only if: the purpose cannot reasonably be established using de-identified data; information released is limited to that necessary; the Research Ethics Committee believes that the benefits of the research clearly outweigh the risk; and the appropriate agreement as to use/disclosure, safeguards and retention/disposal is completed.[256]

In Ontario, a research plan must be submitted to Research Ethics Board and approved before custodian may use information for research.[257] Where the custodian is merely disclosing the information to be used for research, it may only do so where the researcher submits an application in writing, an acceptable and Research Ethics Board approved research plan, and enters into the specified agreement.[258] Similar requirements are imposed in Manitoba[259] and Alberta.[260] Alberta also contains an explicit provision that notwithstanding Research Ethics Board approval a custodian is not required to disclose information to a researcher but may do so and in so doing may impose REB conditions and any additional conditions they deem necessary. This disclosure may or may not require consent, depending on the Research Ethics Board determination.[261]

Ontario also contemplates information may be disclosed to an approved health institute. The health institute is tasked to de-identify the information before using it for health system analysis or disclosing it to the Minister.[262] Additional limits are placed on the disclosure for research to a researcher approved outside of Ontario.[263] Finally, Ontario contains an explicit grandfathering of research uses or disclosures that were begun before PHIPA came into force, allowing them to continue for 3 years.[264]

In Alberta, certain custodians may also use information for the purposes of planning and resource allocation, health system management, public health surveillance and health

[255] Saskatchewan HIPA s. 29(1).
[256] Saskatchewan HIPA s. 29(2).
[257] Ontario PHIPA s. 36(3).
[258] Ontario PHIPA s. 44.
[259] Manitoba HIA s. 24
[260] Alberta HIA s. 50-52, 54.
[261] Alberta HIA s. 53.
[262] Ontario PHIPA s. 47-48.
[263] Ontario PHIPA s. 44(1)
[264] Ontario PHIPA s. 44(12), (13) and (14).

policy development.[265] Information may also be disclosed for systemic purposes, including: an audit[266] as long as conditions are met and an agreement entered into; to enable to Minister to carry out his duties[267]; to the Minister to assist with developing public policy[268].

There are also a number of contemplated systemic uses in Ontario. For instance: information may be disclosed for health or other programs subject to specified conditions being met,[269] for health system purposes where the receiver has in place policies and procedures to protect the privacy and confidentiality of the information and those procedures have been approved by the Ontario Privacy Commissioner,[270] or for the purpose of monitoring or verifying claims for payment for health care.[271]

The concerns regarding the effectiveness of de-identification are raised in the previous section apply equally to data nominally anonymized for research or other purposes. The maturity and capability of the technology should be considered, as data is generally released to new uses and contexts.

With regards to the number of secondary uses contemplated, there is no doubt that the information disclosures can be technologically monitored through authentication, trust and consent management, and that purposes for the release could be logged and audited. However, it is unclear where technological applications are appropriate here. Importantly, some agencies fall outside the reach of the corresponding act and would no longer be subject to these controls on the data. In this case, being outside the "circle of care" relieves them of obligations respecting patient control and autonomy. Although such an agency might still fall under other legislation, such as PIPEDA, it is unclear that any EHR technologies would extend so far.

Maintenance / Retention

Issues of maintenance and data retention influence many of the other rights and duties.

In Ontario, this is addressed by three provisions: that a custodian must have in place information practices that comply with the Act and must comply with those practices,[272] that where a custodian is using electronic means to collect, use, modify, disclose, retain or dispose of personal health information they must comply with additional prescribed regulations,[273] and that a person who provides goods or services which enable a custodian to use electronic means must comply with the prescribed requirements.[274]

---

[265] Alberta HIA s. 27(2)
[266] Alberta HIA s. 35(1)(f)
[267] Alberta HIA s. 40;
[268] Alberta HIA s. 39
[269] Ontario PHIPA s. 39
[270] Ontario PHIPA s. 45
[271] Ontario PHIPA s. 46.
[272] Ontario PHIPA s. 10
[273] Ontario PHIPA s. 10(3)
[274] Ontario PHIPA s. 10(4)

There can be a disconnect between "information practices" and technology – for example, by the Ontario provisions which treat electronic means as a separate category. Effectively, this means that "privacy" and "technology" needs may not be considered together.

Each of the Acts mandates that information must be accurate, complete and up-to-date. In Ontario, Manitoba and Alberta this requirement is couched as an obligation to take reasonable steps to ensure accuracy, completeness and up-to-date status as necessary to meet the purpose before use or disclosure.[275] Saskatchewan makes it explicit that information must be maintained in retrievable, readable and usable state.[276]

A trustee who receives a notice of amendments or annotations that have been made to information previously disclosed to or used by them must make the correlative change to any record in their custody or control.[277] Such changes must not destroy or obliterate the existing information in the record.[278]

While information is retained, reasonable steps must be taken to ensure that records are protected.[279] Manitoba sets out both specific safeguards and additional safeguards, which must be implemented where information kept in electronic format,[280] as does Alberta.[281]

In Ontario there is an additional requirement that the custodian shall make available to the public a written statement detailing a general description of their information practices, the contact information for a representative who can explain any questions, instructions on how to obtain access or request correction of information, and an explanation of how to make a complaint about compliance with the Act.[282] Where the custodian uses or discloses information without consent outside the scope of this description, the custodian must inform the individual at the first reasonable opportunity (unless it is information to which the individual would have no right of access), make note of the actions and keep the note as part of the record.[283] Alberta also requires that policies and procedures to implement the Act be developed[284] and also requires that custodians prepare and submit a PIA describing proposed administrative practices and information systems and have the PIA reviewed by the Alberta Commissioner before implementation.[285]

[275] Ontario PHIPA s. 11. Information that does not meet this standard may be disclosed as long as the recipient is informed of any limitations on accuracy, completeness or up-to-date character of the information. Manitoba PHIA s. 16, Alberta HIA s. 61.
[276] Saskatchewan PHIA s. 17(2).
[277] Saskatchewan PHIA s. 40(5)
[278] Saskatchewan PHIA s. 40(7).
[279] Ontario PHIPA s. 12(1), Manitoba PHIA s. 18(1), Alberta HIA s. 60(1). Saskatchewan HIPA s. 16.
[280] Manitoba PHIA s. 18(2), 18(3).
[281] Alberta HIA s. 60(2).
[282] Ontario PHIPA s. 16(1).
[283] Ontario PHIPA s. 16(2)
[284] Alberta HIA s. 63
[285] Alberta HIA s. 64.

A custodian must ensure that records in their custody or control are dealt with in a secure manner in accordance with the prescribed requirements.[286]

The notion of "reasonable safeguards", however, is problematic in light of ever growing technological capacities. It is difficult enough to determine what security safeguards are reasonable at this very moment. As consent management, privacy rights management and other technologies mature, existing technologies will create legacy problems, it may be difficult or impossible to include improvements in technological capability. Thus, either the safeguards themselves must be "grandfathered" as reasonable or else there is a constant re-design cost in the system. In either case, the end result is that existing technological capacity winds up defining the meaning of privacy.

Ontario explicitly provides that information that is the subject of an access request under s. 53 shall retain the information for as long as necessary to allow the individual to exhaust all recourse.[287]

In Alberta, a custodian may transform individually identifying health information to create non-identifying information.[288] Alberta also contemplates further manipulation of data by allowing custodians to perform data matching on information under its custody or control.[289] Data matching may also be performed by combining information with information held by another custodian[290] or a non-custodian.[291] In either case, before data-matching can take place, a PIA must be performed and submitted to the Alberta Privacy Commissioner. Saskatchewan envisions the creation of a comprehensive health record through combining of records for the purposes of the Saskatchewan Health Information Network[292].

Records may also be combined for purposes other than the creation of a comprehensive health record in Saskatchewan.[293]

These provisions on data linking are clearly technology-driven, responding to the technological capacity to retrieve information from multiple sources. In one sense, they predict the application of data distribution through mechanisms like federated identity management, and suggest a response to the BFHD problem of data aggregation. On the other hand, anonymization research showing information can be re-identified indicates that data linking needs to be undertaking very carefully. In addition, as more information is excluded from the Acts, it becomes freely available for aggregation and re-identification purposes, increasing privacy risk. This problem cannot be fully addressed in a technology and policy regime based on data protection and stewardship.

[286] Ontario PHIPA s. 13(1).
[287] Ontario PHIPA s. 13(2).
[288] Alberta HIA s. 65.
[289] Alberta HIA s. 68.
[290] Alberta HIA s. 70
[291] Alberta HIA s. 71.
[292] Saskatchewan PHIA s. 18.1
[293] Saskatchewan PHIA s. 18.1(4).

Access

Individual access is a key provision of data protection standards. Typically, they require that, upon request, an individual should be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information.[294]

Jurisdictions set out the form an access request must take.[295] In Manitoba a trustee may transfer an access request to another trustee if the other trustee maintains the information or collected it first.[296] In Ontario, before deciding whether to grant access a custodian may consult with selected bodies.[297]

The right of access also puts obligations on the custodian. Custodians must respond fully and openly, including the explanation of terms, codes or abbreviations.[298] Where a custodian is unable to explain, they should refer the individual to a trustee who is able to provide the explanation,[299] a requirement which implicitly carries within it the expectation that the information in a record may have been collected or received from other trustees and that the record will be sufficiently detailed to allow the trustee to identify from whom the information came and thus to whom the requestor should be referred. Although Ontario doesn't provide for such a transfer, a custodian is not required to correct a record where the custodian and custodian did not originally create the record does not have sufficient knowledge to correct it.[300]

Responses must be made within the timelines dictated by the legislation, usually 30 days[301] and should provide access, where denying access, explain why and how to apply for a review, or state that information does not exist or cannot be found.[302]

Alberta provides that where an access request has been received, a record should be created from information that is in electronic form if this can be done using normal computer hardware, software and technical expertise where creating the record will not unreasonably interferes with the operations of the custodian.[303]

Access is the default, but the Acts set out a list of circumstances where access may or must be refused.[304] Where access is refused, information should be severed from the

[294] Saskatchewan HIPA s. 12, s. 32., Alberta HIA s. 7, Manitoba PHIA s. 5, Ontario PHIPA s. 51
[295] Saskatchewan HIPA s. 33-34.
[296] Manitoba PHIA s. 8(1).
[297] Ontario PHIPA s. 52(5)
[298] Saskatchewan HIPA s. 35, Alberta HIA s. 10(a), 10(c), Manitoba PHIA s. 6
[299] Saskatchewan HIPA s. 35.
[300] Ontario PHIPA s. 55(9)
[301] Saskatchewan HIPA s. 36, Alberta HIA s. 12(1), Ontario PHIPA s. 54
[302] Saskatchewan HIPA s. 36, Alberta HIA s. 12(2), Ontario PHIPA s. 54
[303] Alberta HIA s. 10(b), Manitoba PHIA s. 7(3)
[304] Saskatchewan HIPA s. 38, Alberta HIA s. 11, Manitoba PHIA s. 11

record and access to the remainder be provided where possible.[305] In Ontario, certain parts of a record are excluded from the right of access.[306]

The language of access is predicated on the "custody and control" notion that is inherent to records protection rather than to information. Questions arise when these concepts are applied to EMRs. The question of whose custody applies – who has "custody and control" when a record is accessed by multiple providers? Does the access right apply only to information actively maintained by the custodian to whom the access request is directed or to all information to which that custodian has had access during treatment?

In addition, the ability of the patient to manage her data is severely limited by such systems – it is difficult for the patient to gain access to her own information, let alone actively and continuously monitor it. The legislation provides a right of access, but does not effectively support a continuous monitoring given the complex access procedures and requirements imposed. The concept of the PHR – the patient having intimate access to their health information – is simply not supported by this legislation. There is little doubt the technologies of consent management and authentication could extend and even benefit from patient access, but again the patient seems to be outside the "circle of care".

An individual should be able to challenge the accuracy and completeness of the information and have it amended as appropriate.[307] Custodian may refuse to make such a change to certain kinds of information[308] and where such a refusal is made, written notice must be provided to the individual within the time limits setting out reasons for refusal.[309] In Ontario, there is a duty to correct where the individual has demonstrated to the satisfaction of the custodian that the record is incomplete or inaccurate.[310]

In Alberta, where a refusal has been made, the individual may either ask for a review by the Commissioner or submit a statement of disagreement to be added to the record.[311] Where a correction to the information or an annotation to the file has been made, an individual should be so informed.[312]

When a correction to the information has been made or an annotation added to the file, a trustee should where practicable give notice to other trustees and persons to whom the information has been disclosed within the past year.[313] However, under Alberta law no such notification is required where the custodian believes no harm comes to the applicant by virtue of the uncorrected information remaining and the applicant agrees.[314]

---

[305] Saskatchewan HIPA s. 38(2), Manitoba PHIA s. 11(2).
[306] Ontario PHIPA s. 51, Ontario PHIPA s. 55
[307] Saskatchewan HIPA s. 13, s. 40(1), Alberta HIA s. 13(1), Manitoba s. 112(1).
[308] Alberta HIA s. 13(6), Ontario PHIPA s. 55(9)
[309] Alberta HIA s. 13(5), Manitoba PHIA s. 12(3).
[310] Ontario PHIPA s. 55(8), 55(10)
[311] Alberta HIA s. 14(1).
[312] Saskatchewan HIPA s. 40(3), Alberta HIA s. 13(3)
[313] Saskatchewan HIPA s. 40(4), Alberta HIA s. 13(3), 14(3), Ontario PHIPA s. 55(10), Manitoba s. 12(5).
[314] Alberta HIA s. 13(4)

Patient rights to correction of information create liability issues as well as technological ones. Attention needs to be given to how these rights can be operationalized with current technologies without reducing the effectiveness of the chart as a health care tool. How can changes be made meaningful if the original information must also remain in the record? As for annotations/statements, while their inclusion may superficially provide autonomy, are they truly meaningful in shaping the care an individual, or will they simply create liability concerns for physicians? The new technologies should be built to enhance health care, but the effect of some requirements on actual practice is not at all clear.

Disposal

Manitoba law requires that, when information is destroyed, a record be kept of the individual to whom information relates, the date and method of destruction and the person responsible for supervising the destruction.[315] As has been pointed out in other contexts, this type of logging requirement further increases the overhead for record keeping and commensurate privacy risks.

Alberta's requirement to have safeguards for the protection of information mandates that there be safeguards in place to ensure proper disposal of records.[316] Similarly, Saskatchewan's provisions regarding safeguards also include a requirement that information be destroyed in a privacy-protective manner.[317] Ontario not only concurs with this but further requires that where electronic means are used to dispose of information, additional prescribed requirements must be complied with.[318]

These kinds of requirements encourage outsourcing privacy-protection to service providers – the more detailed the data handling requirements, the more likely they will be given over to specialists. While maintaining a semblance of technology-neutrality in the legislation this relegates important technology choices to the operational and implementation level, much of which will end up in the hands of IT industry, with possible different standards in different jurisdictions.

The problem of vague "reasonable safeguards" standards creating legacy technology has already been noted. Combined with outsourcing, the ability of the health care system to encourage the development of improved technology may well be compromised, leaving a situation where the interests of technology vendors and legacy software are controlling the advancement of the field. This is another variation on technological capacity defining privacy.

Breach

Specific obligations when it comes to breach of privacy/security of information are not imposed by the data protection principles, though arguably they may be contemplated

[315] Manitoba PHIA s. 17(4).
[316] Alberta HIA s. 60(2).
[317] Saskatchewan HIPA s. 17(2)
[318] Ontario PHIPA s. 10., s. 13(1)

under the Safeguards and/or Openness principles. Nevertheless, the Ontario legislation contains explicit obligations in the case of such a situation.

Ontario requires that a custodian who has custody or control of personal health information must notify the individual at the first reasonable opportunity if the information is lost, stolen or accessed by unauthorized persons.[319] In the case of a researcher who has custody or control of the information, such contact should only be initiated where the researcher has consent to contact the individuals.[320]

In the case of an agent of the custodian, the agent must notify the custodian at the first reasonable opportunity if the personal health information it handles on behalf of the custodian is lost, stolen or accessed by unauthorized persons.[321] Given that the custodian remains responsible for information under its custody or control when one of its agents performs duties for it, this notification should then set off the notification of individuals' contemplated Section 12.

The notion of information being lost or stolen seems counter-intuitive as a product of the "custody and control" paradigm. The myth of absolute security[322] seems to permeate the legislation, as the breach provisions are minimal at best. That is, although information may be viewed (and thus "stolen") by outsiders, the provisions around consent and authorized access are far more detailed than those around response to a breach, which would lead to speculation that whatever the current state of the art, it is deemed adequate. There are no provisions to actually remediate privacy loss to the individual, just as there are no developed technologies to remediate privacy loss to the individual under the privacy-as-security mindset.

5 Regulations

Regulations are rules created by an administration or administrative agency (often a minister of the government) that helps interpret statutes. The statute may provide the authority to create regulations and set out the administrative body's purpose and powers, or the circumstances of applying the statute. For the purposes of this report, such regulations may provide technology deployment details absent from the statutes. Pertinent regulations from the four jurisdictions with specific health information statutes are:

- Alberta: Regulation 70/2001. *Health Information Act*. Health Information Regulation. (hereafter, Alberta Reg)
- Saskatchewan: *The Health Information Protection Regulations*, Chapter H-0.021 Reg 1. Effective July 22, 2005. (hereafter, Saskatchewn Reg)
- Manitoba: *The Personal Health Information Act*, C.C.S.M. c. P33.5. Personal Health Information Regulation 245/97. Registered December 11, 1997.

[319] Ontario PHIPA s. 12(2).
[320] Ontario PHIPA s. 12(3).
[321] Ontario PHIPA s. 17(3).
[322] see page 42

Amendment 142/2005. Registered September 30, 2005. (hereafter, Manitoba Reg)
- Ontario: *Personal Health Information Protection Act,* 2004. Ontario Regulation 329/04, Amended to O. Reg. 537/06. (hereafter, Ontario Reg)

B.C. also has some relevant provisions in regulations under its Privacy legislation:

- *Freedom of Information and Protection of Privacy Act*, Freedom of Information and Protection of Privacy Regulation B.C. Reg. 323/93. Effective October 4, 1993. (hereafter, B.C. Reg)

The following sections consider the contents of these regulations under the general topic categories used to review the legislation.

Collection

British Columbia and Saskatchewan's regulations contain no provisions related to collection that specifically include technological requirements. Ontario and Alberta's regulations are predicated on assumptions about technological capacity, including the: opportunity to provide electronic consent; opportunity to revoke consent electronically; ability to collect enough information for authentication; ability to link authentication information to consent / revocation requests; and the ability to grant and revoke consent.

Ontario's regulations Section 6(3)4 is predicated on the same assumptions as the Alberta requirements with respect to the identification of logging requirements. Section 8(1) provides exceptions to the authorization requirement, with notifications to patients for unauthorized collection. Ontario's regulations also provide for grandfathering of consent requirements.

Manitoba's regulations provide a more detailed set of assumptions about technological capability, including the ability to maintain a record; ability to record and log user activity; ability to connect record end user activity; prior to this, the assumption of access to electronic health information; ability to maintain an electronic health system; ability to identify the user, record and accesses; and the ability to accurately collect these logs. Section 4(1) further assumes that PHI is actually stored electronically by designated trustees. Section 4(2) assumes that logs can be generated, and there is sufficient support to do so manually or electronically. Section 4(3) provides for exceptions to logging, which are essentially policy decisions.

The technological assumptions respecting collection are essentially design requirements for an electronic health system. They are high-level abstract descriptions, created by the legislature; not necessarily by those directly involved with the provision of care. While there is still some interpretive scope for those implementing the e-Health systems, it is clear these criteria will be influenced by the current implementation environment: budgets, administrative restrictions, and technological capability. Technology to meet these requirements exists, but they may be burdensome in terms of expense, reporting and oversight, for which the supporting infrastructure may not exist (such as resources,

funding, training and in some cases, interest in compliance). Technologies within this scope include user authentication, user authorization, access control, and consent management.

Provision of Access

Saskatchewan, British Columbia and Alberta's regulations contain no specific technological requirements for provision of access. The Ontario regulations that speak directly to the role of a health information network provider (HINP) (defined as an electronic service provider to two or more health information custodians, or clinicians) require that they restrict access to electronic PHI unless they have sufficient technological safeguards in place. These are not defined.[323] Section 3 of Manitoba's regulations provide requirements regarding PHI protection, including access, storage and removable media handling, but do not refer specifically to electronic health records. Removable media requirements are restricted to secure storage.[324]

In this case, technology exacerbates the risks associated with the access to PHI through the data aggregation problems noted elsewhere. Although there is some specific language, references to secure storage and undefined safeguards do not add significant details to evaluate particular security or privacy technology, and do not provide much more specifics than the general language provided in various pieces of legislation. It does provide clarity with respect to some aspects of the authority and responsibility for data handling.

Technologies implicated in this include access controls, authentication and data management and data aggregation. Where technological developments move at a faster pace then policy, privacy and security requirements associated with provision of access may not be reflected in legislation unless and until issues have arisen.

Use

Manitoba, British Columbia, Alberta and Saskatchewan's regulations contain no specific technological requirements relating to use of personal health information. Ontario's regulations for HINPs place limits on the use of PHI in the course of providing electronic services; restricting them to that which is necessary for the provision of the service.[325] This may or may not include additional technological practices, such as logging, auditing and/or monitoring, that are part of best security practices in technology environment.

Like the statutory provisions, there is little guidance as to the extent or the specifics regarding the electronic services to be provided, or the particular means of restricting use of the information, the technical means of monitoring or how the authority to use the data is to be exercised. Where these specifics are probably impractical to provide in primary legislation, it might be possible to include more specifics in regulations, since they are

[323]Ontario Reg, section 6.
[324] Manitoba Reg, section 3
[325] Ontario regs, section 6.

more easily modified to suit the evolution of electronic services. Implicated technologies may include access control, data encryption, data authentication, and user identity management, but specific guidelines for applying these technologies is not provided in regulations.

Secondary Use

Most of the provincial legislation and associated regulations provide such a broad definition of use that secondary use provisions are not needed to support the data management and administrative activities of their institutions. For example, there are up to 11 permitted uses of PHI that are implicitly embedded in a patient consent document. Ontario[326] provides for the custodial use or otherwise access to PHI for research, insurance and risk analysis purposes and by specific public health organizations, and Manitoba[327] includes conditions for the review of projects using PHI.

These provisions generally infer that a patient admitted to the hospital has consented to treatment, and consequently part of any research or public health initiatives engaging the PHI collected at the hospital. Thus, consent management mechanisms have to account for the statutory authority for the provision of PHI for secondary use. Where the provisions are often unclear is how the outside agency (often not being a custodian) will have to enagage similar technologies. That is, there is no indication that the research or public health body will have to use the same or similar consent management system or similar technology as the hospital.

Disclosure

British Columbia and Manitoba regulations have no mention of disclosure provisions and/or restrictions that specifically mention technological elements. Alberta's regulation section 8 (6) require custodians of PHI, and their affiliates, to adhere to all technical safeguards associated with PHI. Saskatchewan regulation section 5(1)(ii), requires ministers upon disclosure for quality of care related work to deidentify individual health numbers or other unique identifiers, with a unique encrypted identifier. This assumption is predicated on the existing of such technology, and then the framework to support electronic data aggregation is in place.

Ontario regulations require that HINPs do not disclose any PHI to which they have access a result of providing electronic services to custodians (clinicians). Section 18(8) makes specific mention of the electronic master person index, allowing prescribed entities to disclose PHI for the purposes of organizing and accurately identifying people contained in the electronic index. This is a clear allusion to the Infoway-style registry architecture.

These regulations reflect a technology bias towards the de-identification by removing identifiers, and are subject to the weaknesses in effectiveness of de-identification techniques associated with the related technology.

[326] Ontario regs, sections 13, 14, 18(3), 25(2).
[327] Manitoba regs s. 8.1.

Retention/Maintenance

British Columbia, Alberta and Saskatchewan's regulations contain no mention of retention and / or maintenance requirements for personal health information. Manitoba's regulations set out a specific retention schedule for logs of user activity on systems that contain PHI. In addition section 2 provides that: there is a written policy in place to support the enforcement of the safeguards in place for protecting the electronic PHI; PHI will be stored electronically; that the storage media is removable; and that the storage media may be disposed of, and/or used for certain other purposes[328]

Breach

Manitoba's Personal Health Information Act Regulations section 4(4) require a trustee of PHI to conducting ongoing audits to look for security breaches. Ontario requires electronic service providers specifically to notify custodians of any access, use, disclosure or disposal that is unauthorized or inappropriate.[329] Alberta's regulations (section 8(7)) require that custodians establish sanctions, and impose them, against individuals who breach or attempt to breach, the technical safeguards associated with electronic PHI.

Computerized PHI systems import all of the above listed requirements for breaches and associated handling procedures. No technology can ultimately guarantee to prevent breach. Heuristic scanning technologies that can examine access patterns for attempted intrusions are in constant development, as many other technologies mentioned in Part I of this report. There are no specific unrealistic or burdensome technology-related expectations, but at the same time there is no specific response to increased data aggregation risks.

There are a number of technologies associated with breaches of electronic PHI; ranging from consent management to data storage management. Each technology introduces risks of unauthorized and inappropriate access, use and disclosure. Rather than setting out specific requirements for breach procedures and/or reporting, regulations often set out provisions about safeguards and logging. The policy, such as mandatory notification requirements, seems to attempt to mitigate the associated privacy harms. In some regulations, the dual use of access logging data to identify attempted intrusion and well as actual intrusion is clearly articulated.

Investigation

Instead of setting out specific requirements for investigative procedures and reporting, regulations often set out provisions about safeguards or logging. Alberta regulations section 8(1) require custodians to identify and maintain written records of technical safeguards associated with electronic PHI. Custodians are further required to identify and designate an individual responsible for information security; in addition, they must

[328] Manitoba regs Section 2.
[329] Ontario regs,Section 6(3).

complete assessments of technical safeguards, including any reasonably anticipated threat, as well as any unauthorized use, disclosure or modification. Manitoba regulation section 2 requires written policies and procedures to document provisions for recording breaches and corrective actions. Section 4(3) provides exceptions to logging, for example, electronic transfers between custodians and information systems. Ontario's regulations require electronic providers to provide plain language descriptions that including a description of the technical safeguards in place. In addition, providers are required to document and distribute threat, vulnerability and risk assessments of the services provided to custodians. Written agreements are required to outline the technical safeguards.

The technology has resulted in the development of legislative requirements largely about documentation of technical security safeguards. In this case, there is a privacy risk associated particularly in the technology environment as investigations tend to become more about the event, such as data forensics, than they are about the perpetrator. While this can yield improvements, it does not combat of new kinds of intrusion attacks. Nor does it address mediation of the effects of the privacy violations of successful attacks. The implications mainly affect those outside the circle of care, such as regulators and administrators. Those inside the circle of care would be more affected by the original breach, as opposed to the ensuing investigation.

Technologies that are implicated in investigations are typically management function tools: audit, logging and monitoring. This reflects the fact that administrative policies within institutions tend to operate in a reactive, rather than proactive manner. Often, the development and implementation of legislation or procedures reflect problems uncovered by breaches once they have already occurred. The policies relating to *notification* about a breach are generally related to the development of corresponding technology. This implicitly recognizes that breaches in *electronic* records may be significantly more extensive and broad reaching than paper records.

6 Privacy Impact Assesment

6.1 Introduction[330]

A PIA provides an assessment of whether a proposed program, policy or legislation has any privacy impact or compliance issues with respect to existing information privacy legislation. (including PHI) is handled. The assessment process may also include consideration of other types of privacy issues[331] that pose a threat to the success of the overall project.

A PIA can be applied to any project that handles personal information. The project may be any proposal, review, system, database, program, application, service or agency initiative. A completed PIA can be used to design a program, policy or legislation in a way that mitigates any privacy impact as far as possible. Thus, a PIA has institutional benefits: helping to find privacy solutions which also support the project's goals; identifying the potential for future privacy impact such as function creep (uses of information which evolve away from original expectations) or new legislation or technology; improving the project's public and stakeholder consultation; demonstrating that the handling of personal information in the project has been critically analysed with privacy in mind; and educating throughout the appropriate institutions regarding privacy.

The Treasury Board Secretariat (TBS) PIA policy applies to 150 federal institutions that include Government of Canada (GoC) departments, agencies and a number of Crown Corporations, and offers a consistent framework to use when identifying and resolving

---

[330] This section of the report relies on a number of pan-Canadian assessment resources, including the following: Canadian Institute for Health Information, Privacy Toolkit, October 2003. Available online at http://secure.cihi.ca/cihiweb/en/downloads/privacy_toolkit_binder_2003_e.pdf. Alberta Medical Association, Office of the Information Privacy Commissioner (Alberta) Resources. Available online at http://www.albertadoctors.org/bcm/ama/ama-website.nsf/AllDoc/F5AD2D7F915F53CF87256E8C006D3827?OpenDocument. Office of the Information Privacy Commissioner (Alberta), Registry of Privacy Impact Assessments (Searchable Database). Available online at http://www.oipc.ab.ca/pia/registry.cfm. Office of the Information Privacy Commissioner (Alberta), PIA: Description. Available online at http://www.oipc.ab.ca/pia/. Office of the Information Privacy Commissioner (Alberta), PIA: Templates. Available online at http://www.oipc.ab.ca/pia/template.cfm. Government of British Columbia, Ministry of Labour and Citizen's Services, Privacy Impact Assessment Process. Available online at http://www.lcs.gov.bc.ca/privacyaccess/PIA/PIAprocess.htm. Office of the Information Privacy Commissioner (Ontario), Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act. Available online at http://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf. Canada Health Infoway, Electronic Health Record Infrastructure (EHRi) Privacy and Security Conceptual Architecture. Available online at http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf. Canadian Health Infoway, An Overview of the Electronic Health Record Privacy and Security Conceptual Architecture. Available online at http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security-Overview.pdf. Centre for Health Information Newfoundland and Labrador, Request for Proposals for Professional Services Standing Offer to Conduct Privacy Impact Assessments of the Newfoundland and Labrador Diagnostic Imaging / Provincial Archives Communications System and other Electronic Health Record related projects. Available online at http://www.nlchi.nf.ca/pdf/PIA_RFP_Dec15.pdf.

[331] There are other types of privacy, e.g. bodily privacy; territorial privacy; communications privacy.

privacy issues during the design or re-design of programs and services. It has provided a model and rationale for the use of PIAs which is nationally recognized:[332]

> The Privacy Commissioner has publicly endorsed PIAs as a means of ensuring the protection of Canadians' personal information. Canadian institutions have conducted privacy assessments for a number of years and have taken steps to ensure the protection of Canadian citizens' privacy in their transactions with government.

The framework is based on PIPEDA's ten privacy principles and represents the first time a national government has made conducting PIAs a matter of official policy. Subsequent provincial legislation typically adopted requirements for assessments on any government initiative that may affect an individuals' privacy, often comprising PIAs or Threat Risk Assessments (TRA) for security, and privacy assessment.[333] Many agencies are also subject to agency-specific legislative requirements that add further privacy protections (such as secrecy provisions), as well as legislative requirements that apply generally across government.[334]

---

[332] Treasury Board of Canada Secretariat, Privacy Impact Assessment: Policies and Publications. Available online at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp.

[333] see Ontario's *Personal Health Information Protection Act*, 2004 (PHIPA), Regulation 329/04, as amended 537/06, section 6. Available online at http://www.e-laws.gov.on.ca/DBLaws/Regs/English/040329_e.htm.

[334] Information regarding PIAs related to legislative privacy oversight are listed here by jurisdiction as follows: **Oversight Jurisdiction**, *Legislative Governace Bodies;* online PIA resource:
Federal Privacy Commissioner: (http://www.privcom.gc.ca/);Treasury Board (*http://www.tbs-sct.gc.ca /tbsimScripts/topic-sujet-list_e.asp?ID=121*), Justice Canada, Industry Canada; http://www.privcom.gc.ca/information/index_e.asp.
Federal Information Commissioner: (http://www.infocom.gc.ca/menu-e.asp);Treasury Board (*http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_121/siglist_e.asp*), Justice Canada, Industry Canada; http://www.infocom.gc.ca/media/default-e.asp.
BritishColumbia:(http://www.oipcbc.org/);IM/IT Privacy and Legislation Branch (*http://www.mser.gov.bc.ca/privacyaccess/*); http://www.oipcbc.org/resources.htm
Alberta:(http://www.oipc.ab.ca/home/);Information Management, Access and Privacy Division (*http://foip.gov.ab.ca/*) Alberta Health and Wellness (*http://www.health.gov.ab.ca/about/Minister_legislation.html*);http://www.oipc.ab.ca/publications/.
Saskatchewan: (http://www.oipc.sk.ca/);Saskatchewan Justice (*http://www.saskjustice.gov.sk.ca/foi/default.shtml*); http://www.oipc.sk.ca/resources.htm.
Manitoba: (http://ombudsman.mb.ca/access.htm); Manitoba Health (*http://www.gov.mb.ca/health/phia/index.html*) Access and Privacy Services of the Government Records Office at the Archives of Manitoba. (*http://www.gov.mb.ca/chc/fippa/index.html*) ;http://ombudsman.mb.ca/resources.htm
Ontario:(http://www.ipc.on.ca/);MGS, Access and Privacy Office (*http://www.accessandprivacy.gov.on.ca/english/*); http://www.ipc.on.ca/index.asp?navid=8 .
Quebec: (http://www.cai.gouv.qc.ca/index-en.html);Ministère des relations avec les citoyens et de l'immigration.
Nova Scotia:(http://www.foipop.ns.ca/);Department of Justice (*http://www.gov.ns.ca/just/*);http://www.gov.ns.ca/foiro/pub_admin.html.
Newfoundland and Labrador: (http://www.oipc.gov.nl.ca/) ;Department of Justice (*http://www.justice.gov.nl.ca/just/*);http://www.oipc.gov.nl.ca/resources.htm
New Brunswick: (http://www.gnb.ca/0073/index-e.asp).
Prince Edward Island: (http://www.assembly.pe.ca/index.php3?number=1013943); Attorney General (*http://www.gov.pe.ca/foipp/index.php3*).
Yukon: (http://www.ombudsman.yk.ca/infoprivacy/info_index.html);ATIPP Office (*http://www.atipp.gov.yk.ca/*).
Northwest Territories: (http://www.assembly.gov.nt.ca/OfficeOftheClerk/StatutoryOfficers.html);Department of Justice (*http://www.justice.gov.nt.ca/ATIPP/atipp.htm*).

A PIA helps to identify and make any necessary adjustments during a project's development, so that it will comply with all relevant laws that relate to the handling of personal information. A PIA can include a list of applicable privacy laws and an account of how the data-handling practices of the project, as well as the business rules to carry out those practices, will comply with specific provisions.

6.2 Classifications

PIAs vary in their focus and level of technical detail. Three general kinds of assessments are described below.[335]

Conceptual: A conceptual PIA is used to analyze the implications of the idea behind a particular proposal or initiative. It should be completed as part of the project feasibility study so that the results may feed in to the established mechanisms for balancing business constraints with technology constraints to produce a cost-effective solution that enables (or, minimally, does not harm) the individual's expression of their privacy rights.

Design: The concept of a 'design level' analysis originates with hard sciences, e.g. engineering. In privacy, this level of analysis typically refers to the level of detail found in data flows, and the corresponding privacy analysis. For example, a design level analysis could include technical architecture diagrams indicating the flow of PHI between firewalls. A typical finding could include a statement about the access privileges of a particular type of database administrator.

Implementation: This kind of assessment typically examines options for implementing a specific solution, e.g. in the case of applications, the choice of one versus the other, from a privacy perspective. One of the criteria might be which contained the most 'privacy friendly' options. Alternatively, an implementation level assessment could also be done on, for example, an application that has already been chosen. In this case, the PIA would serve to recommended strategies and options for enhancing the application's implementation to enable an individual to exercise their privacy rights.

The exact composition of PIA contents is dependent on the context and institutional requirements. A typical breakdown of PIA contents is provided elsewhere.[336]

6.3 PIAs and Health Care

The introduction of the PIA into the healthcare environment is predicated on the electronic nature of information management and information technology practices of

---

Nunavut: (http://www.gov.nu.ca/Nunavut/atip/);Department of Executive and Intergovernmental Affairs;http://www.info-privacy.nu.ca/en/faq

[335] Distinctions are based on a number of PIA resource related documents, including Canadian Health Infoway's Privacy Impact Assessment resources, available online at http://knowledge.infoway-inforoute.ca. Treasury Board of Canada Secretariat, Privacy Impact Assessment: Policies and Publications. Available online at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp. Canadian Institute for Health Information, Privacy Toolkit, October 2003. Available online at http://secure.cihi.ca/cihiweb/en/downloads/privacy_toolkit_binder_2003_e.pdf.

[336] see online document http://cpig.cs.mun.ca/PIAchart.pdf

personal heath information. The legal rules, ethical guidelines and professional etiquette that govern and guide traditional communications between the health care clinician and patient are equally applicable to email, Web sites, list serves and other electronic communications. However, the technology of online communications introduces special concerns and risks. The reminder of this section examines the how PIAs address these concerns under the same categories used to examine PHI legislation. It generally takes the approach of a conceptual level PIA, as the most general of the kinds of PIA identified.

Collection[337]

An assessment would touch on concepts of direct collection, [338] for example, where a clinician directly asks a patient for PHI and inputs it directly into an electronic medical record. An assessment should also consider the possibility of indirect collection, for example, where PHI is taken from a source other than the individual.[339] A PIA should also consider practices that may be contrary to established privacy rules on managing collection, for example, to ensure that the stated purpose for collection and the actual practice of collection are consistent.

Generally speaking, custodians must collect PHI directly from patients or clients (e.g. by asking questions) and with their consent (which may be express or implied).[340] Following legislation, indirect collection is permitted but in limited and specific circumstances. Persons may collect on behalf of the custodian are agents of the custodian (e.g. a technician who is employed by the hospital) where authorized by the custodian and subject to the same legal guidelines.

There is an acknowledgement in health privacy across Canada that the multitude of legal, regulatory and accreditation frameworks have resulted in a number of subtle variances across the country in the application of assessment methodology:

> Governments across Canada have expressed their commitment to the protection of personal information. This commitment is particularly relevant in the context of efforts to identify, develop, and implement electronic service delivery applications to improve customer service. Where such efforts involve cross-or multi-jurisdictional service delivery, the protection of personal information may be complicated by a number of factors, such as differing legislative frameworks, or variations in public expectations.[341]

---

[337] Also includes concepts related to consent management practices.

[338] Collection refers to the act of gathering PHI from the person to whom it relates. See Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 79.

[339] Concepts of direct and indirect collection are based on Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 79.

[340] Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 79.

[341] Ontario Ministry of Government Services, Access and Privacy Office. Model Cross Jurisdictional Privacy Impact Assessment, Draft. October 1999. Available online at http://www.accessandprivacy.gov.on.ca/english/pub/fed_pia.pdf.

PIAs tend to be based on the PIPEDA/CSA code and business practice standards such as ISO 17799. This is predictably a result of the PIA's function within the organizational business and project processes, providing evidence of due diligence. While actual or defacto standards have a positive role, they also may reduce the PIA to a pro forma 'tick in the box' exercise.

The PIA raises once again the issue of informed consent in an electronic health care system. A clinician is responsible for being able to explain – at the moment of collection – the information management practices that will be used to handle a patient's PHI. In this sense, technology creates and exacerbates the collection risks, suggesting custodians need to be able to communicate technical architecture in a meaningful way. This kind of informed consent also requires the patient to understand electronic information management practices; individuals must be made aware of information management practices that exist in support of their electronic records. IT service providers should produce information about the product / service and its data flows in plain language for the health care provider to give to the patient. It further adds technical requirements to document and manage consent at the time of collection in support of the embedded technologies.

For a hospital or other large organization this may include the need to provide training on PHI and technology to a large staff, auditing activities of a database administrator, defining the 'minimum necessary' rule for collection in the development of applications, and providing other design advice and support for the technology. A variety of technologies are implicated, including user authentication, access control, consent management and logging.

Even without computerized health care system, custodians would still need policy statements relating to both direct and indirect collection. Technology complicates these requirements. Traditional privacy friendly collection practices require custodians to explain and notify patients adequately of purposes and information management practices, a task that is substantially easier when all files (in the case of a doctor's office) are stored internally, or where (in the case of a hospital) there is a health records management department. This promotes aggregate data solutions with their associated risks.

Provision of Access

A PIA typically deals with access by examining how users are credentialed, [342] including the business processes and data flows associated with instructing and retrieving PHI from electronic systems. Access must be consistent with the purposes for which it was collected.[343] In the case of health care partnerships, e.g. shared clinical repository or an

[342] Access to PHI refers to the ability and / or right to engage in some activity with the data. Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 78.

[343] Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 79.

electronic health record across multiple sites, access to PHI originating fro m another custodian should not be accessed for reasons other than care without the patient's express consent. In the case of service providers (e.g. an office cleaning service), custodians are responsible for ensuring that access to PHI is restricted to the minimum necessary to provide services, which would typically mean by contract and enforcement.

Individual custodians (private clinics) who access the information also retain responsibility for ensuring the integrity and accuracy of the information, whereas healthcare organizations that employ clinicians share the responsibility. For example, an organization is responsible for showing due diligence in educating clinicians about accessing PHI electronically. Technology has clarified the liability for information technology and information management by putting it in the hands of the custodian (be it organizational or individual). Custodians are now responsible for procedures that manage technology risks. For example, standard email services are not secure. Custodians need to be aware of any risks, and guard against them with technologies such as automatic logout and password protection. The custodian is also responsible for facilitating a patient's right of access and correction to their PHI. This includes any records relating to electronic information management practices that capture PHI: logs, audit trails, access monitoring records, and backups.

Use

A PIA deals with use[344] from a business perspective, e.g. auditing the business practices and data flows of PHI contained in an electronic system to ensure use practices consistent with legal, regulatory and accreditation requirements. Assessments are typically based on two key principles associated with use: (1) Custodians are limited in the use of PHI by the consent provisions and identified purpose for collection; and (2) Custodians are required to abide by any requests by patients to limit disclosure of defined portions of their health record where appropriate in the provision of care mandate.[345]

Those within the circle of care become incident managers in the event of an external unauthorized use, or auditors in the event of internal unauthorized use. Outside regulatory bodies can be challenged by unreported internal instances of unauthorized use of technology systems that contain PHI. From the patient perspective, it is difficult to prove that PHI has been used.

Within a technical environment, the custodian must take steps to protect patient privacy and to guard against unauthorized use of patient information, extending to contracts with an electronic service provider. This includes developing provisions in the contract

[344] Use of PHI refers to the application and / or analysis of the information for a given purpose, in this context, typically the provision of health care to the patient whom the information relates. Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 84.

[345] This may be a patient right that was specifically enacted as part of provincial PHI legislation. The CSA Code in the PIPEDA does not provide clear guidance on the patient's right to limit disclosure of their health record.

relating to limitations of use of the PHI. The custodian must implement reasonable steps to authenticate the identity of correspondent(s) in an electronic communication and to ensure that recipients of information are authorized to receive it. In addition, the custodian is responsible for ensuring that access can be prevented where requested by a patient.

Secondary Use

Secondary use essentially refers to situations where data is being used for purposes other than those for which it was originally collected. Concepts of secondary use in PHI generally relate to use for the purposes of health research, but also refer to administrative planning, health management and payment for services.[346] A PIA deals with this for assessment purposes, e.g. is PHI accessible by someone other than the custodian of the data? In some cases, depending on who is doing the assessment (internal or external auditors), a PIA could also cover secondary use by the custodian, highlighting those that exist beyond the direct provision of care to the patient to whom the data relates.

The role a PIA plays in assessing secondary use is often limited. The secondary use of PHI is not always identified during the assessment or at the time of data collection. This can be dealt with through gathering additional consent from the patients, or (more conveniently) through the implicit consent requirements set out in privacy and health privacy legislation.

There are few technical controls in place to limit how clinicians handle their patient data for research purposes. Having patient data on an electronic system facilitates this kind of secondary use, which may or may not be appropriate.

A PIA can reveal other secondary use issues that may or may arise as a result of technology. Technology itself introduces a number of other (potentially legitimate) 'uses', e.g. logging, monitoring and auditing of the technology infrastructure to ensure its integrity. Electronic information handling practices might conceivably require additional consent. For example, consent to provide care is given to the clinicians, not a database administrator. Such uses are commonly subsumed into the technology, and implicit consent or necessity may be used to justify them.

These types of risks impact those outside the circle of care, such as research bodies. Researchers who use electronic patient data are obligated to appropriately d`e-identify while maintaining the integrity of the data electronically, put in place appropriate electronic safeguards, follow appropriate and legal retention and destruction processes (including backups and logs). Other roles impacted include regulatory bodies, such as Research Ethics Boards, who are responsible for ensuring appropriate privacy protections as part of the approvals process for projects, including the information technology and management practices associated with a given initiative.

[346] Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 83.

Disclosure

A PIA can highlight possible risks for unauthorized disclosure[347] or make recommendations for limiting access where appropriate to support the business decisions behind a given product, service or initiative. Custodians are responsible for handling all requests for disclosure. Custodians are also responsible for complying with response times, and assessing the appropriateness and necessity of the disclosure.

The risks associated with disclosure, e.g. incomplete records, incorrect addresses and/or incomplete transmissions, can be actively lowered by the use of different technologies. Logging and monitoring can reveal instances of inappropriate disclosure. The custodian is also responsible for advising patients of potential privacy risks associated with such logging and monitoring. These issues are mostly of concern to the patient, and those within the circle of care, such as clinicians, who are providing direct care to the patient and are therefore in most urgent need of complete and accurate records in a timely fashion. With efficient and effective technologies in place (as assessed by a PIA), PHI can be disclosed electronically quickly and accurately to support the provision of care. This disclosure to another clinician requires them to take on the liabilities associated with information technology and information management of a given patient's health records. A doctor's responsibility for appropriate disclosure includes service providers who may have access to his / her electronic information systems.

Retention / Maintenance

Retention and maintenance of PHI records refers to a schedule with the directions on how long records are to be kept, usually by series, for example, for a period of years, until a given project or activity is complete, or indefinitely.[348] It may also include instructions on when records are to be transferred to archives, or destroyed. An assessment highlights the possible risks relating to PHI record management, on all media including backup tapes and logs.

Health records are subject to retention schedules as prescribed by legal, regulatory and professional accreditation requirements, electronic systems of health records often create unknown series of data, for example, if an application log contains PHI, it is considered a health record. Backup tapes of electronic health systems are considered health records; as are documents created to provide support processes to applications that contain PHI (if, for example, they contain screenshots of a problem.) Related concerns of unauthorized collection, access, use and disclosure would be highlighted as risks in a PIA. These types of privacy risks for mainly affect those outside the circle of care, such as regulatory bodies and managers within the organizational context.

[347] Disclosure refers to the release of a patient's PHI to anyone or any organization that is not the primary custodian. Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 80, 84.

[348] Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 83.

PHI records, logs and audits, are considered (generally) the responsibility of the custodian. This would include retention schedules of all associated electronic PHI. In the event that custodians opt out of the electronic record, records would have to be replicated so that each custodian would have a complete set of records of all patients seen. This may or may not be consistent with existing privacy legislation (in terms of meeting the limited disclosure and collection of the minimum necessary requirements.) In other words, there may be no practical way to opt out. The nature of information technology infrastructure and architecture requires a more comprehensive data identification and policy application to control manage and meet the legal obligations associated with each custodian.

Disposal

Disposal practices refer to a set of instructions, and / or a formal authority, that sets out the length of time a given PHI data series should be destroyed.[349] It may also include directions for specific disposal practices. A PIA will take these concepts and apply them to a given project, product and / or initiative to ensure that disposal practices are accurate, actively in place, appropriate, and consistent with legal and regulatory requirements.

The custodian has responsibility for secure disposal of all associated electronic PHI. Guidelines are typically set in a contract and / or service level agreement (in the case where the custodian is a healthcare organization), e.g. backup tapes will be destroyed in a secure manner consistent with industry standards for sensitive and highly confidential information. Discreet retention of the data in a facility specific format facilitates this severing / destruction of the data. The specific technology concerns here relate to efficient and effective backup and support processes, as a preventative measure. Information technology infrastructure and architecture complicates these processes. For example, multiple data sets outside the original record can result in incomplete destruction practices, with attendant compliance risks.

Breach

A breach refers to a violation of a law, right or duty, either by commission or omission, including any failure to fulfill an obligation or condition of a contract.[350] A PIA plays no specific role in breaches, except to provide reference documentation of the system, and evidence of any pre-existing privacy risks.

A breach can cross institutional boundaries, typically the domain of security personnel, and internal boundaries, typically the domain of privacy personnel. Internal intrusions could be highlighted as risks, and addressed (at the risk identification and preliminary management phases) through a PIA and associated recommendations. Instead, choices are often left to incident managers, policy people, and operational staff within a

[349] Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 83.
[350] Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 78-79.

healthcare organization to handle on an ad hoc basis through incident management and incident response planning.

Investigation

An investigation relating to PHI refers to a systematic, minute and thorough attempt to determine the facts of a given incident, situation or breach.[351] It can be informal or formal, official or unofficial, conducted internally, externally (e.g. by law enforcement) or by an independent audit firm. While this might be considered a secondary use of logging data, an assessment has no specific role to play in conducting an investigation, although it may support information gathering and related processes.

7 Conclusion

7.1 Using the legislation

A review of this legislative landscape provides some basic conclusions about the data stewardship paradigm in health care.

Recognizing the broad scope of health care provision, which health care providers are involved identify the statutes relevant to data stewardship. When dealing with health care practitioners, the private sector privacy legislation and the health-sector specific privacy legislation are the most relevant. However, in situations where other bodies (including, in some cases, regulatory authorities) are envisioned as part of the circle of care, it may be necessary to consult the applicable public sector privacy legislation as well.

Operationally, it should be noted that many of these statutes fall within complementary jurisdictions, meaning no one statute will necessarily cover all instances of data collection, use or transfer. PIPEDA is often described as "a floor, not a ceiling", meaning that more stringent protections might apply than those called for in the legislation. The main concern, however, is striking the right balance between privacy rights and the "greater social good" pursued in the sharing of PHI.

Regardless of the "privacy" language employed in the legislation, the invocation and adherence to the 10 principles of the CSA code makes it clear that these pieces of legislation are, at their root, about data management. They seek not to protect a right of privacy, but rather pursue the business orientation of codifying the responsibilities of organizations with regard to personal information that they collect, use or disclose, as well as prescribe standards for data management while it is in the custody or under the control of organizations. This is not, of course, incompatible with privacy rights, but it may leave questions about what actual privacy rights are recognized.

[351] Canada's Health Informatics Association (COACH), Guidelines for the Protection of Health Information. (Toronto, Ontario). 2001. Page 83, 84.

7.2 Technology Implications

There is a real move towards technologizing health care provision. Unfortunately, some important implications can be missed in the rush to develop policy to meet the needs of burgeoning technological expansion. This review of the technological implications of current Canadian health privacy legislation indicates the following overarching concerns:

Technology-driven legislation

Despite the legitimate effort to create technology-neutral policy at the legislative level, (to be interpreted at the operational level), clear influences of existing technology assumptions can be detected. The data protection/stewardship paradigm for privacy itself is embedded in the context of the development of security technologies in the business world. In other words, the perimeter model and privacy-as-security mindset behind the current technologies are about data protection, and so is the legislation. This may be a sensible reaction to deploying the only mature software technologies available, but it is important to recognize it is a policy direction, not a law of nature. Technologies that operate with different assumptions, as suggested in Part I of this report, *could be* developed.

There are also some specific references to registry systems, limitations to opt-out or withdrawing PHI, data linking provisions, and statements regarding de-identification that appear to be concessions to current technological limitations, rather than simply good policy choices. These can be particularly hazardous if they tie current legislative policy to particular technological limitations that may disappear in the future – leaving legacy systems that cannot be adequately re-tooled. Compounding this feature is the tendency to leave specific choices and definitions of "reasonable safeguards" to individual system designers or EMRs. Even if industry norms evolve, they are likely to create legacy problems in the future once a stable interoperative EHR infrastructure is developed.

Conceptual weaknesses

While co-opting the notion of privacy rights, these statutes instead function to regulate data stewardship and effect data protection. Under this regime, numerous statements which purport to extend an individual's autonomy in the guise of data protection may instead function to restrict it. This includes not only reliance on implied consent or consent exceptions, but the assumption that consent when proffered is meaningfully implemented in technologies like consent management, authorization, privacy rights management or trust management. If the technology deploys consent directives based on roles the patient does not control and implemented in trust management mechanisms from which the patient (or custodian) cannot withdraw their trust, the meaning of concepts like trust and consent have been compromised.

Part of these difficulties can arise if concepts from technologies – such as the circle of trust, or trusted third party, are misapplied to health application concepts, such as the circle of care or custodian. Superficially, the concepts appear related, but the reality of which party *actually* controls and secures the data may be determined by the

technological implementation, not the "custody and control" relationship described in the legislation. The intended relationships between service providers and custodians, for example, may indeed hold, but they are *not* enforced by conventional privacy and security technologies (nor is anyone building such enforcement technology) – some other enforcement mechanism is necessary.

Some clarity is needed around the question of what provisions the technology will actually enforce or be responsible for. Current identity management, authentication, access control and consent management technologies can implement disclosure provisions and attempt to enforce them by preventing inappropriate access. Use and collection provisions could be monitored through surveillance oriented technologies of logging and auditing (although it is doubtful even that much is contemplated in most systems). Does policy contemplate the development of technologies for enforcement rather than simply monitoring of useage and collection provisions? Is it intended for all of the possible purposes, decisions and useage directives be logged and monitored? If so, the amount of logging and auditing implicated is staggering. Merely logging of access itself (which is the conventional approach) creates privacy risks due to the creation and maintenance of ever-increasing bodies of information.

Access to and control of information

The language of the legislation is directed towards existing security and privacy technology because it is directed to data records rather than information. Custody or control of a record is not control of information itself. By focusing on protections at the records-level, these laws fail to fully interrogate or protect privacy of health information, relying instead on the management of health records. Equating a circle of care to a perimeter of records custody makes it difficult to assess exactly how privacy is protected.

De-identification as a means of privacy is similarly problematic. Taking de-identified data outside the scope of these acts ignores the uncertainty that surrounds anonymzation technologies regarding re-identification. Ongoing technological developments and the increase in information logging and data aggregation all contribute to the possible problems in this area.

The consent model that is fundamental to informational self-determination is weakened by legislated exceptions to consent and technologies that may provide limited consent based on defined custodial roles. The definitions of custodian and PHI may restrict legislative rights, but it unclear that the technologies for trust, identity management, authentication, consent management actually employ these distinctions, since the actual custody and control relies on the persons furthest from the circle of care – the service providers –behaving in a trustworthy manner.

Finally, some clear delineation of policy regarding patient access and the PHR vision should be articulated, since the overly complex rules of access to information and the strictures around access provide little clarity as to a patient's rights in this regard. The legislative focus seems to be building EMRs and EHRs, not PHRs.

Part III: Comments from Stakeholders

This part of the project surveys the concerns of stakeholders with the deployment of security and privacy technologies in the health care system. This is not an attempt to draw a representative sample and identify statistical or normative trends in the beliefs or attitudes of stakeholder groups. There are a number of studies which accomplish those ends.[352,353,354] Instead, more in-depth and less formal interviews were held with a select number of participants, allowing issues to be pursued in more depth as they arose. Without a rigorous methodology for participant selection or the structure of the interview items or process, the ideas and opinions are presented on their own merits.

As with the rest of the report, the discussion concentrates on concerns with privacy issues or mismatches between expectations and technological capacity. There is no attempt to balance these with positive experiences or an analysis of whether EMRs/EHRs are delivering on improved health care. Indeed, it is not difficult to find numerous anecdotes of positive benefits and experiences of front-line workers with the adoption of EMRs.[355] Although these are not pertinent to this project's agenda, the reader should not be left with the impression that positive outcomes do not exist.

There are also notable biases in the participant selection. The primary care providers, for example, are exclusively represented by physicians with some experience dealing with EMRs. There are no pharmacists, dentists, lab technicians, nurses, or other primary care provider roles represented. This was partly due to the response profile to the call for participation, but also tempered by the fact that physicians appear to be the most involved in addressing individual patient information in EMRs. Some of the individuals interviewed have in fact designed, built and operated EMRs in clinical practice over many years. Even more striking, there is no representation by patients – the very persons whose privacy is at stake. In fact, the entire arena of development and deployment of EMRs/EHRs appears to be bereft of patient advocacy. Sadly, the later material in this section suggests that patients are not engaged or well enough informed to participate meaningfully in the discussion.

Nonetheless, the material does provide an interesting cross-section of important stakeholder groups, and the results indicate many areas of general agreement as well as differing perspectives both among and between groups of stakeholders. There are no doubt elements that are overlooked with this approach, but it does try to connect

[352] *e.g.*, Pullman, D. and Power, A., (2006) "Sorry, You Can't Have That Information: Stakeholder Awareness, Perceptions and Concerns Regarding the Disclosure and Use of Personal Health Information." Presented at *Electronic Health Information & Privacy Conference*. Available online: http://www.ocri.ca/ehip/presentations.html.

[353] EKOS Research Associated Survey on the Pan-Canadian Health Information Priavcy and Confidentiality Framework, 2006

[354] also see footnote 387

[355] Ontario's Smart Systems for Health has a web page of anecdotes: http://www.ssha.on.ca/success-stories/index.asp

observations regarding privacy-related technologies and the legislative privacy framework with actual experiences in the health care sector.

The interview material is divided roughly into four groups – oversight, policy administration, technology development and marketing, and primary care provider. These categories are rough in the sense that they encompass both comments by stakeholders described by the category and comments by others directed to that category of activity.

In each category, the material is divided into various perspectives on the meaning of privacy in the health information, technology deployment, and the relationship between policy and technology.

Participants are identified by letter-designation in Appendix A.

1 Oversight

There are a number of oversight bodies which operate in the privacy arena in health. In terms of procedures and rules, legislation typically creates responsibilities for institutions or custodians to respond to complaints or inquiries, and places oversight for these responsibilities on a privacy commissioner or ombuds-person within the jurisdiction. The relevant legislative oversight office depends on the governing jurisdiction, which is not always clear due to the mix of public, private and health-specific legislation noted in Part II of this report. Although this group represents legislative oversight, it should also be noted that there can often be a variety of other bodies with oversight responsibilities, such as professional licensing boards (some of which are beginning to look at IT issues in detail)[dd]. This can create a confusing mix of obligations.

Different oversight agencies may have different scope in terms of their oversight responsibilities. For example, some jurisdictions require conduct of a PIA when new health information infrastructure is deployed. This may involve some degree of independent review of system design and architecture documents [f] or simply receipt of a filed PIA. [d] In others, the oversight body may limit itself to responding to complaints and inquiries, and leave the assessment of the new infrastructure to the institutions or authorities responsible for health care delivery. This appears to be an issue of governance capacity, as much as it is deliberate policy.

There is some oversight attention given to vendor conformance and specific compliance standards for technological solutions. The level of the oversight entity involved varies between jurisdictions. In some jurisdictions, there is a specific agency undertaking this kind of work, some staff this responsibility in the provincial privacy commissioner's office, while others leave technical details to the individual health care agencies.

Personnel at these offices are not only in the position of interpreting the legislation and considering compliance, but also struggle with the effectiveness and impact of privacy rules and legislation. This section should illustrate some of the issues that arise at this

conceptual level regarding the appropriateness of technology application with respect to privacy.

1.1 The Meaning of Privacy

The most common articulation of privacy surrounding personal information in health is that of "the right to control information about yourself", which adheres to the literal statement of the Supreme Court [356]

> …we talk about it [privacy] in terms of informational self-determination and the way we approach it is we want to maximize whenever possible, a citizen, consumer, a patient's personal control over who they give their information to and how that information is used and disclosed ***- Mary Carlson*** [e]

> … the traditional definition is the individuals right to control the collection, use and disclosure of their own personal information. That's related to individual control and choice and self determination, but it's also more about fair information practices and how the organization allows the individual to exercise their right to privacy ***- Debra Grant*** [q]

However, there is a clear recognition that the strict notion of informational autonomy is insufficient to completely encompass privacy concepts. The limitations of data protection and fair information practices as expression of autonomy or privacy is understood:

> I think there are three concepts that are at play here the privacy sort of serves but are more fundamental then privacy. One is the notion of autonomy that is very strongly connected to data protection … data protection is about me exercising my capacity to control the information …and the idea of dignity, privacy serves dignity, it serves self respect and the worth of a human life and you know the right to a private life and things like that that are independent of the idea of autonomy … and I think a third one that is worth mentioning to is the idea of liberty in the sense that you're… allowed to be free from government surveillance, intrusion, big brother … we use the word privacy as somehow a word that describes all three of them but really they take priority on the basis of different situations – ***Avner Levin*** [x]

So privacy is narrowly engaged as autonomy, and autonomy is rather obliquely interpreted as data protection. After all, even if someone has no autonomy (if the legislation or health care technology gave them no real choices), there could still be legislative rules and practices to protect PHI and keep their identity private.

Some commentators would make further distinctions among privacy (information controlled by oneself), confidentiality (control of information shared with other parties) and data protection (obligations relating to protecting data) as being different

[356] "…the right of the individual to determine for himself when, how, and to what extent he will release person information about himself,…" R v. Sanelli [1990] 1 S.C.R. 30

conceptually and legally.[357] As rules for data protection, the legislative framework and health information specific acts incidentally protect confidentiality and privacy in their broadest sense.

> The legislation which is called Personal Data Protection, that legislation is neither about confidentiality nor privacy. It's about giving control of information about a subject, to that subject. It's not about privacy, because it absolutely assumes that the information is disseminated through an organization that's covered by the legislation. It doesn't fit into the traditional definition as informational autonomy. It tries to impose… an effect on collection. And it does! It says that in the best circumstances you will get information about an identifiable individual, from that identifiable individual. But it isn't the legislation that mandates the collection, it says if you're going to collect, you must collect from this person, but it doesn't say to this person, "you must disseminate to that organization."
>
> - ***Margaret Ann Wilkinson*** [mm]

Under this interpretation, information doesn't even have to be *about* the individual to be a matter of privacy – it simply has to originate with the individual. [mm]

If privacy's proxy is data protection, it operates through legislative mechanisms of consent, agency (in the case of service providers or those outside the "circle of care"), and permissive rules on collection, use and dissemination based on legitimate purposes. Data stewardship becomes a surrogate for confidentiality and privacy. EHR and EMR technology follow this same course: substituting consent management, authentication processes and technical provisions of good data handling practices for actual privacy. Information is not controlled by the patient, but by an interlocking arrangement of consent directives and exceptions, statutory obligations, and technology safeguards over which the patient has little direct control.

It is important to tease out the differences in these concepts. Confusion over what is privacy, security or confidentiality can lead to inactivity in operationalization of privacy policy, as it become difficult to assign roles, responsibility and accountability within an organization.

The balancing act necessary for the handling of PHI is crucial to the oversight mandate. It is recognized as being especially sensitive, even sacred, and at the same time having to be shared to be useful. [d,e,x] "Protecting patient confidentiality is about establishing a working and healthy relationship between patients and health care professionals … if patient care is compromised by privacy then maybe we've got the tail wagging the dog" The trick is finding a way to "meet the privacy and security intent at the same time not slowing down their efficiency to such a state it will hamper their ability to provide good quality care." [d] This dilemma permeates new system design and legacy system problems: "its really important to have the information available to the right person at the right time. Systems have been designed that way and its really hard for those systems to

[357] Wilkinson, M.A. "Privacy and personal data protection: Albatross on Access", in Karen Adams and William F. Birdsall (eds.) *Access to Informaiton in a Digital World.* Ottawa: Canadian Libray Assoc. 109-132

be retrofit now with the new privacy regulations that are coming into effect and the new reality about privacy and how information is becoming more vulnerable to security breaches, identity thefts, hackers and also its use for other secondary purposes, employers, insurance companies, things of that nature" [q]

1.2 Technology deployment matters

Technology is recognized as both the source of the privacy risks and the potential solution:

> … on the one hand it can pose a threat but on the other hand it can also help us to mitigate some of the risk to privacy so you have audit trails, anonymization technologies, encryption. So on one hand you have this accumulation of information which is like a jackpot for anybody who wants to use it for an unintended purpose, employers, insurance, governments, researchers, and it can also be used for other purposes like those of identity thefts and rogue employees who want to sell the information. – ***Fred Carter*** [f]

But there is recognition that technology is not a panacea. People are ultimately the biggest security and privacy problem, whether it is poor physical security around passwords or looking over peoples' shoulders, or the insider stealing data they have access to, that cause the privacy violations. [f] If individuals do not secure their passwords, none of the privacy-related technologies will defend against breaches.

1.2.1 Aggregation

The BFHD (page 43) risk is also recognized. Computerized data aggregation and networking is seen as an issue, partly because "putting things in great big databases will only increase risks… someone can go in and steal all the files or they can burn it with digital data they can steal a gigabyte of information in a second and send it all around the world and you would never even know that the theft occurred … this is the flipside of the ease and convenience of large databases and networks… the security and the integrity and the confidentiality represent real and genuine risk because the more valuable [the data] then the more you have to start replicating it" whereas "you know if you break into a doctor's office that's paper based you can maybe run off with a couple of files." [e] The incentive to centralize expertise and data protection, reinforcing aggregation of data, is also recognized. [f]

1.2.2 Logs and Logging

Logging is seen as one of the most important technologies available, because it creates an audit capability that simply doesn't exist with traditional records. "…strong auditing capabilities leaves a clear footprint of who has accessed your health record…with paper records that is something that is very hard to do." [d] But it is not entirely clear how to handle all this data, or protect it when it includes PHI. "… now you've got personal

health information all over the place in these logs." [f] Certainly technologies like FIM [358] can help alleviate this problem, but clear policies as to what log data constitutes PHI and how it should be protected are needed.

1.2.3 Access control

Authentication as access control is seen as a central to controlling people's rights: "you link all those databases, you link lab and drug and diagnostic imaging into EMR into public health surveillance, back into the health authorities the first question is .. how do you meaningfully control access into a system like that because now you have the capacity to show the complete view of a human being and not everybody is entitled to everything that's in there" [e]

There are some questions whether the role based approach will flexible enough, whether it will provide the granularity of control desired, or even what that granularity is. This comes down to whether particular fields can be protected separately from entire records, [q] so that patients can allow certain people access to part of the record. In RBAC, this becomes a matter of defining roles correctly.[359] For consent management, the question becomes whether adequate types of consent are available for the user.

1.2.4 Consent

Questions arising over the dependence on consent as a mechanism for privacy (typically cast as autonomy) are at once conceptual and technological.

Consent has a great deal of complexity associated with it in the health care context. A tendency of consent to be diluted across different forms of consent in law (such as implied or deemed consent) was noted, as the ability of individuals to withhold consent is balanced with the need to provide health care.

One concern is whether individuals meaningfully give an informed consent in such a complex technological environment, without knowledge of the risks and technology deployed. It is suggested that users have no problem trusting the system until their attention is drawn to those aspects that may be of concern. "Privacy is something you cherish only when you've lost it. " There is a power relationship to consider. "in a healthcare context you know you're going to the physician for health care, are you not going to provide the consent if the physician tells you that they need it in order to provide you with the healthcare…so its meaningless to talk about getting the consent in that sort of ideal way that the data protection commissioners envision" [x]

Explicit provisions do attempt to address concerns around meaningful consent. In Quebec, for example, depositing medical information in regional data banks is subject to informed consent. [ff] If "consent" is not freely given, then in some real sense the extensive use of undermines confidence in the system rather than increasing it. [x] Implied

[358] see page 33
[359] see page 21

consent should mean the information is volunteered in circumstances in which the exposure of the information is clearly understood. This would not usually include migration of the data into a repository for future use. The technology challenge should become building "transparency … so a patient understands really what's happening to their data so that they know what's going on with it so they can properly participate in the discussion about it… maximize the transparency and do things like allow patients online access to the log to see who has accessed their data" [e].

There is tension between this view and the idea that consent, once given, would encompass the entire "circle of care", as a practical issue in provision of health care. Otherwise, consent would have to be acquired over and over again, with privacy rights explained at each instance.

In other words, even if the consent management mechanisms are deployed, the legislative exceptions and practical limitations in monitoring consent may simply mean that technology capability creates an illusion of patient autonomy.

This recalls the basic question of whether consent is a proper way to engage privacy (even when understood as autonomy) in the data stewardship context: "In these health personal data protection legislation, the statute actually says, if the medical practioners believe that its in the best interests of the patient that there be an implied consent, then there's an implied consent. Well that's a different statement, that's the old professional care model. And that is really talking about confidentiality, because its saying you're going to trust the care professionals to keep the information within the circle of care." [mm]

Withdrawal of consent highlights the same mis-match between consent as articulated by technology and legislation and the notion of personal autonomy in information. Once data has been diffused and shared throughout the health care system, there is little capacity to withdraw the data in any significant way. (And so much of the legislation doesn't provide for withdrawal, but uses notification instead.)

1.2.5 Patient control

The nature of consent relates to the question of the extent to which patients are in control of their health information. "Its the expectation that we're going to build in strong identity management and access control. We're going to give patients control over their data somehow, we're going to audit" [e] "I'm always looking for maximum patient involvement in the control and management of their health info… if I were to sit down and design my dream system it would be one where the patient could but with very little additional effort and with high security and great convenience pull up a file on them" [f] The PHR vision of instant auditing by the patient simply isn't contemplated by legislation,[360] (or current designs [v]) and the difficulty of implementing even the annotation rights and the withdrawal rights that exist are recognized.

[360] see page 79

There is a paradox of sorts here: while the health sector legislation moves away from patient control of their data through mechanisms like implied consent, [mm] and as an alternative creates stringent rules for data sharing, it is conceived as increasing protection and patient control. There is little doubt this double-think is enabled by the technology capabilities to do consent management, trust management and authorization controls.

1.2.6 Circle of care

Part of the loss of autonomy or control is due to the notion of the circle of care or teams in providing health services. Health care has become increasingly about information sharing among teams and less about an individual caregiver's expertise. [mm] This raises question of where to draw the line of data-sharing, which is not always satisfactorily answered by the legislation. People are comfortable with their specialist and personal physician, but the further you move away to allied health professionals, the more leary they become of data sharing. [e] Within this circle, there are still consent and authorization concerns, which makes the burden significant if the technology is expected to track, monitor and provide audit trails for these relationships.

There is an intuition that the correct perimeter is those involved with the provision of primary care, but it is not always clear, how far things extend when billing, lab reports, and private service providers begin to enter the picture. This can be particularly difficult for patients to understand.

The notion of a custodian helps define limits, but even combined with legislative rules and technology there is no standard definition of who is inside or outside the circle. [aa] It is often the service provider that is handling the data through an agency or contractual relationship. "who's is the repository of that information? .. it can't really be the custodian because they really don't have control over anything other then their little piece that they put in it" [q] In other words, even if the "circle of care" or custodianship or "team" is nominally restricted to the primary care providers, in practical and technological terms the data is secured by another party. If they are not inside the circle, it is difficult to see how the concept is effective. As noted in Part II, (see page 63) the technology security perimeter does not map precisely onto concepts like the circle of care or the legislated distinctions.

1.2.7 Secondary use

One of the great values of EHRs is the capability they will provide for secondary uses including research and health surveillance. "there's a lot of pressure to leverage that information and use it for publicly beneficial purposes, research and planning, managing the system and all those secondary uses so you have to decide what are legitimate uses.. the information has always been used for other purposes its just that .. people are being more transparent about it" [q]

Anonymizaiton of the data is one approach to secondary use, which takes the data outside the scope of legislation defining PHI as personally identifying information. It can be difficult to decide when this line is crossed, and the data is truly de-identified. It also

often ignores the problems associated with re-identification: "if we have information which has been disassembled so that the personal identifier element of it is not known, but then it is recontextualized in a way that re-introduces the capacity for personal identification, at the time that new context is created and that personal identification exists, if somebody asks for then, you have to be able to retrieve it, and it comes within the act."[mm] In other words, it is difficult to determine when something can be re-identified and becomes subject to PHI rules again. Current anonymization technology does not target this problem – it anonymizes the data and "sets it free", handing it to non-custodians. [361]

It also ignores the nature of the research or surveillance activity itself. "The legislation is not actually looking at the anonymization of the research product, it's looking at the anonymization of the record. People are confused about that." [mm]

There's a further confusion in that the new legislation is placing obligations on research uses that displace existing exceptions for research. "universities are so geared to the ethics office, and actually these issues are no longer a matter of ethics or Tri-Council guidelines, but are actually legislated. But the institutions are not making the connection, so strange things are happening." [mm]

Technology really doesn't respond to any of these concerns – the anonymization technologies can be measured according to some risk factors, but the actual use of the data, once it passes outside the scope of legislation, could potentially be out of the scope of the privacy technology as well.

1.3 The relationship between policy and technology

A key question for this report is whether technology is leading policy decisions. While legislation is meant to be technology neutral, it is technology choices that ultimately determine the level of data protection available. Rules that address specific technology risks are needed to build public confidence.[u] Commissioners are starting to articulate more regarding specific technology choices [e] and understand that technical decisions, that is the actual technology deployed, will have a huge impact on the effectiveness of governance models and their costs. [e]

There is a belief that basic principles of fair information practices are not affected by technology choices. [q]. A few simple principles, according to some, can guide the adoption of technologies. [f] On the other hand, choices have to be made and there is a reluctance to be an early adopter of PETs or other advanced technology. "… nobody wants to be the first to implement them… I know there's some good stuff that's in prototype and that people are talking about and trying to promote but they're not out there being used now so it would be a leap of faith for them to say let's bring in this [new] anonymization technology. It just doesn't happen…… it requires a champion of that

[361] see page 75

technology and somebody at a high level who has influence and power needs to decide this is the way we're gonna go, otherwise it just doesn't happen." [q]

This is sometimes seen to be the role of policy or legislation, to create pressure to introduce new technology or retrofit the existing technology. However, when the legislation creates difficulties for technology, there is recognizable pressure to adapt the law. "the technology shouldn't dictate the privacy policy and there's a lot of pressure in Ontario to get rid of the lock box requirement … that allow the individual to opt out of their implied consent… but because of the technology there is pressure to change the policy but hopefully that's not going to happen."[q]

Sometimes the legislative intent is simply not implementable, or not feasible in a cost effective manner. Flexible control by the patient over levels of consent, directions of information flow and the subject matter they are going to permit remains impractical. The building of the record then remains in the hands of the professionals, not the patients. [mm] While the legislation may be met through a combination of technology and other elements, in practice the technology may not be responsive to the legislation.

There is some concern the attempt to sustain policy that is technology neutrality creates problems. At the oversight level, one suggestion is that legislation and regulation are too wordy and hard to interpret in the context of specific technologies. The amount of effort required to "just to make sure that people are actually understanding what is required of them in different situations" [x] is problematic. Adherence to simple principles and their interpretation in the context of specific technologies might be more effective.

Some believe that more fine-grained advice about technology is needed, not only to provide guidance to deployment, but also to indicate what is actually being deployed. People need this information to actually understand the technology to which they're consenting. [f] There is a lack of interpretive rules about specific rules about standards, particular technologies, and question such as IP protocol numbers constitutes PHI or not. The question of whether *consent* information is *health* information, for example, may determine which piece of legislation applies – the health specific rules, or the more general PIPEDA.

To some extent, specific technology decisions belong at the operational level – with tools like the privacy impact assessment. But there are concerns that PIAs simply don't ask the "hard questions" about privacy risk, that they are more about compliance with a standard check list of requirements and less about privacy. There are also positive comments that the Inforway project is leading improvement in this area, with the advocacy of conceptual PIAs. [e] Warnings include the comment that risk analysis is an ongoing activity, not a one-time effort, and organizations need to be held to that expectation. [f]

1.3.1 Incremental approach

A popular perspective says that policy and technology go hand in hand: policy must respond to effects of technology as it is deployed,[362] but technology must also be implemented in response to new policy directions. This fits well will the Infoway program which envisions incremental adoption of technologies over time. To some extent an incremental approach is inevitable, as there will always be day to day complaints and practical problems to be resolved, and the need to engage in real public debate about policy choices. [q]. Legislation will constantly need to be updated, as IT changes.[ff] To some extent this leaves technology leading policy development, with little guidance for the early adopters, who are unclear whether what they are trying to achieve will be acceptable under future policy regimes.

1.3.2 Business approach

A further concern with the existing PIAs and risk analysis approaches is importing a business-oriented approach which may not be an appropriate fit to health care. They "tend to emphasize the risks to the organization rather than the risks to the individuals… so in the case of a data breach you'll have a protocol that looks at all those risks and mitigates those risks… but in the event of a data breach the biggest risk could be deemed the risk to the reputation of the organization". [f] The economics of information security may not create sufficient protection for the individual PHI, and may fail to speak to trust or confidence of the public, so it is all the more important to include statutory protection, with provisions like notification-on-breach.[u]

Organizations generally don't want to engage in-depth analysis of general principles: they want turnkey solutions and clear answers. Therefore, the incentive is to use standard solutions and existing applications, not to engage complex PIAs with conceptually challenging questions.

One of readily-challenged assumptions in the EHR business model is that the data has to move substantial distances. While the value of moving data in the local "circle of care" is increasingly obvious, it is less clear that there is a need for health information to travel out of province, or that the ability for instantaneous access to large datasets at long distances doesn't come at the cost of other values [mm] such as autonomy and confidentiality. The largest value of a large pan-Canadian EHR system may be the advantages it provides by enforcing a standard of local interoperability: "if you don't use a pan-Canadian approach, you are definitely not going to have systems that speak together when they have to… and interoperability within a province is of great value that we've seen already.. " [dd]

[362] "..you won't understand [all] implications [of new technology] unless you are actually faced with a situation which is close to real; you can only anticipate so much" [ebJR]

1.3.3 Mutiple authorities and jurisdictions

The relationship among data repositories and service providers is difficult to handle when it is responsible to multiple jurisdictions or multiple custodians with different policies: "the wait times information system is actually being operated by Cancer Care Ontario on behalf of the health information custodian so they're acting as agents … so there's really, really complex relationships and those need to be worked out." [q]

Similar confusion may arise about what law applies, as noted in the legislative review. This creates even more complexity when multiple jurisdictions become involved (such as data being shipped across borders to service providers or other EMRs)., and oblilgations to professional organizations and codes of practice,[363] with their own complaint procedures are layered on top of custodial obligations in legislation. In responding to so many oversight bodies, custodians have a tremendous administrative task, and must rely on harmonization of rules and procedures to make their information environment manageable.

This translates into technology problems as well: for example, two jurisdictions with different consent models may not be able to share data, [v] and sophisticated PRM technologies can be attempted to manage data sharing: but PRM will likely reduce data sharing.

While the importance of harmonization between jurisdictions is understood, and many standardization discussions and efforts do take place, Canadian oversight bodies tend to work independently. The rules at this level tend to be like the legislation – attempting to prevent committing to any particular technology. The practical elements that actually affect the ability to talk across jurisdictions or to multiple authorities is therefore not decided at the level of legislation where it is enforced, but at the lower level of operational implementation. In the meantime, information and privacy breaches are inherently borderless, so the risks cannot be compartmentalized like the systems can.

While there is a need to make policy that is independent of any particular technology, it is problematic when policy may be left to interpretation by IT specialists. This can lead to a tendency to "outsource" aspects of the problem or place them into simplistic categories such as "security" versus "privacy" which maybe poorly communicated. If the goals in the rules of legislation are left to information handling or data stewardship, then it is difficult to assess outcomes in terms of improvement to patient privacy.

1.3.4 Public trust and confidence

Although there are public concerns with exposure of records and cross-border exchange of information, there is a general belief that large scale security breaches by intruders are not as large a concern as inappropriate access by insiders – from the "browsing" or "over the shoulder" observation of records. [e]

[363] e.g. Canadian Medical Association's *Health Information Privacy Code*, online at: http://www.cma.ca/

The consensus seems to be that patients are more interested in who is looking at their data than the actual content or access mechanisms. Few patients actually want to annotate their file, but it is important to know who's been accessing the data.[f]

Faith in the system is also important from the health care provider's side. "Consumers, physicians and hospitals espouse very different cultures around the acquisition, mining and management of personal health data." [s] Doctors may refrain from data entry if they don't believe it has benefits for the patient, or it creates problems for their own privacy. Furthermore, there is some expression of concern regarding patients locking information away from the treating physician.[e] Different cultures of what's important makes it difficult to build community around data sharing and PHI management.

Part of building this trust is bringing tangible benefits to the primary care system, and delivering on the promises that have been promulgated for this technology. [f] "For consumers, particularly those facing significant health challenges, health data related issues around control, convenience, ease of access, and improved health outcomes are probably more important than privacy and security." [s]

The privacy legislation can be seen not only as a substitution of data protection as a proxy for privacy protection, but a shift in the way trust and confidence operates in the system. Trust develops foremost with the primary care provider,[x] which can be challenged by legislation which diffuses responsibility for the patient's confidential information. For example, while the doctor is still responsible for the custody and control of records housed by a service provider, its not clear how the custodian doctor can effectively ensure safeguards are in place or observed. [e]

While there is a belief among some that audit and access controls for patients will be the means of building such trust, little attention is given to the shift in emphasis this places within the system as a policy matter. In one sense, the patient is being asked to trust the system rather than their health care provider, and it is reasonable to question this approach.

The use of access controls on those inside the "circle of care" for example, inherently suggests they should not be trusted. Should this reduce patient concerns about access or heighten them? There does appear to be an unquestioned assumption that replacing this trust with access control mechanisms is a positive use of technology, which may need to be challenged: "The answer lies not in increasing electronic security measures…building a fortress around personal health information…but rather, through vigorously reinforcing the culture of respect for patient privacy." [364]

[364] Geiger, G. (2006) "Privacy Considerations During the Implementation of Electronic Health Records." Presented at *Electronic Health Information & Privacy Conference*. Available online: http://www.ocri.ca/ehip/presentations.html.

Peekhaus[365] examines the extent to which some legislation includes privacy rights in their data protection schemes. Alternatively, one might suggest that the regime is attempting to supplant confidentiality with data protection. In the meantime, it is not clear to what extent the physician now relies on others in fulfilling the professional obligation to protect confidential information - technology deployment and data protection legislation may have reduced his or her ability to exercise this obligation.

Finally, there is an issue that the human may be simply better at protecting an individual's confidence than a computer system. Privacy risk is very contextual – for example, living in a small town creates different nuances around disclosure than living in a large city. [s, u] Computer systems tend to respond well to predetermined rules, not to individual nuances that create exceptions.

2 Policy Administration

In this section, issues are examined from the institutional policy perspective, with comments from individuals with a broader mandate, including regional health authorities and health care agencies. While broadly characterized as policy administration, some of these individuals spend more time implementing policy on a daily basis, while others help institutions interpret policy.

The PIPEDA requires an organization to have a privacy officer to deal with the administration of their privacy responsibility. Generally speaking, there are administrators in this type of role for health care agencies – whether it is a regional health care authority, hospital or crown corporation with a specific health care mandate. These individuals are generally responsible for interpreting the legislation and rules for their organizations.

Some policy administrators belong to organizations that have a strong commitment that the technology is or can be effective. While there may be a large concern regarding privacy risks, as with the oversight agencies, these may often be viewed as a matter of public perception than real. [dd] The common view is that privacy concerns can be respected, while accommodating the advantages of access for primary care, public health surveillance and research purposes. It is a matter of getting the technology right, and deploying it properly where it can be effective. Of course, there are instances of technology being rejected for it inability to properly protect PHI. [b] Lessons and technology can be drawn, with appropriate caution, from the business world. [dd] The operational problem is one of correct program delivery: matching legislative demands with technological understanding and making sure the right communication and representation is involved in the process. [dd]

The privacy policy administrator's role is generally to ensure institutional compliance with the rules and regulations applicable to their institution under the relevant legislation. They typically direct the institution's adoption and use of risk management methods and

[365] Peekhuas, W.(2006) "Personal Medical Information: Privacy or Personal Data Protection?", *Canadian Journal of Law and Technology*, June 2006.

PIAs. If new EMR or EHR technology is being deployed, these are the officers of the organization that examine the implications for privacy and ensure that the institutions react appropriately. The privacy implementation challenges for the organization fall on their shoulders.[366]

The administrator views technological responses as one possible avenue to responding to a risk or obligation. In other words, a particular obligation or risk can be addressed through a variety of means: electronic, physical, educational, establishing new protocols or infrastructure, and so on. [y] A technological response may be an appropriate response, or it may not. Technology is not viewed as having changed the nature of privacy, as underlying principles remain the same.

A great deal of institutional guidelines and standardization had grown up around the data stewardship approach, which helps define the obligations and lays out appropriate institutional responses. Organizations like COACH create detailed guidelines[367] based around common standards such as the CSA model code, the ISO 17799 and the incorporation of the same principles into PIAs and other instruments. While valuable tools, these do not lend themselves to analyzing new emerging relationships between technology and institutional practice – they tend to be recipes capturing the knowledge and experience of practice in the data security and data protection fields. For a regime focussed on data stewardship, these do not directly address patient privacy.

2.1 The meaning of privacy

Privacy as personal autonomy is recognized, but the language of data protection is more common with some mention of the notion of confidentiality as a supporting element of privacy.

It is noted that there is some tendency to focus on data protection and technologies and policy measures that are already in place. Patients should know what is happening with their data, and assert right over its control (including collection limitations, corrections, and so on) according to the legislation that is in place to protect them. The rules provided though the legislative instruments and the CSA code are central to this viewpoint. As one might expect, the notion of privacy is defined in operational terms by those dealing with operational tasks, which tends to fit the notion of data stewardship. Supporting the custodian's control and custody is central, which translates to creating a secure and private electronic infrastructure.

There is also a tendency to separate privacy and security matters. Security issues are often relegated to an IT implementation problem, since they do not involve roles inside the organization: some administrators tend to see data theft as a security issue, for

[366] Curtis, J. (2006) "Information Privacy and Security Implementation for Healthcare: Policy, Process and Progress." Presented at *Electronic Health Information & Privacy Conference*. Available online: http://www.ocri.ca/ehip/presentations.html.

[367] COACH (2006) *Guidelines for the Protection of Health Information*. Available for purchase online: http://www.coachorg.com/default.asp?ID=439.

example, unrelated to the rules and procedure internal to an organization – the custodial privacy issues.[y] This separation between security and privacy might not be pertinent to a patient, for example, and is not the same as the proposed distinction based on technologies in Part I (page 14).

There are acknowledgement that attempts to address privacy as a technology problem is limited – there are too many social and contextual complexities.[368] The fact you've been attending a physician may not be sensitive – until she is revealed to be a Psychiatrist. Innocuous facts about clinic visits are meaningless, until someone discerns the pattern of AIDS treatment among the data. There is some argument that values of privacy have been traditionally protected by the health worker, and technology response should be limited to traditional security risks – that is, data theft.

2.2 Technology deployment matters

Particularly among this stakeholder group, there is recognition that the system ultimately relies on humans – that physical safeguards are needed, and ultimately the technology is managed by people. Must more pragmatic concerns arise – for example, making sure appropriate security was in place for wireless "floating information" in particular was mentioned.

A desire for greater capability to implement and track consent was also expressed, which is seen as a response not only to existing rules and legislation, but due to the differing levels of sensitivity and tolerances with respect to health information.

As there is concern over "scope creep", the capability for aggregated or linkable data collections to provide more and more information about an individual: "Identifiers are very powerful tools and the more technology systems we have and the more they need to be integrated and talk to one another those identifiers have the potential for linking disparate systems … it's not a bad thing, I just think we need protections around the use and collection and purposes for those identifiers"

Controlling data sharing is a recognized principal, as well as being articulated in legislation. The Infoway vision limits the amount of patient information traveling through the geographically dispersed EHRs, suggesting most patient information will be localized in EMRs. [dd]

2.3 The relationship between policy and technology

While policy implementation and technology deployment are seen as an integrated activity, there is a clear perception that policy leads the process or should lead the process. It provides the framework in which administrators operate. Administrators see their role as implementing or interpreting existing policy.

> Legislation and policy must be translated to technology. Policy mitigates the risks

[368] see footnote 364.

> and technology reflects whatever is included in the legislation. Policy comes first …The lock-box, for example, is a policy concept that has to be translated into technology. In response individual service providers have to conform to this new policy.
>
> … technology is an enabler and I think privacy policy needs to be developed in terms of the objectives and purposes for collecting personally identifiable information first and foremost and then you can see how technology can help you. I think that sometimes we put technology first.

While dictating very specific technology introduces concerns of being overly prescriptive, the policy needs to clarify what should happen in the electronic environment. A problem arises when technology outstrips existing policy . "Technology moves a lot faster than policy, making policy development is a difficult thing. Development of rules at the operational level are problematic (around network access from home, use of email, flashcards, wireless devices in the workplace) as the technology advances so quickly." The concerns revolve around policy for specific technologies – blackberries, networking, use of personal computers outside the institution. Technology is moving so fast it is seen by some as the driving force, rather than a supporter of the process.

Certainly there can be resistance to technology adoption when security concerns so indicate. In at last one district networking was determined as unsafe, and users are encouraged to use encrypted laptops for health information rather than relying on networked communications.

2.3.1 The business approach

Technology choices are imbedded in an institutional, business-oriented model: "The biggest risks to privacy is how to balance the business needs with the production of privacy and understand that there is a reason for identifiable personal health information or … anonomized personal health information to support a certain business need".

The administrative approach to new technology projects traditionally treats security and privacy as secondary to the features or functionality of the system, sometimes not even appearing in initial requirements for a project. Security and privacy concerns have become better understood as fundamental, rather than being an afterthought in the deployment of systems.[369]

Security and privacy requirements are usually determined through risk assessment and PIAs based on standard resources like the CSA model code and ISO standards 17799/27799. Where the CSA code and its progeny provide general principles, the ISO17799 is more specific – "a comprehensive set of controls comprising best practices in information security... intended to serve as a single reference point for identifying a

[369] Cavoukian, A. (2005) "Privacy by Design: Don't Make Privacy An Afterthought – Build It In." Presented at *Convergence Expo 2005*. Available online: http://www.ipc.on.ca/index.asp?navid=46&fid1=13.

range of controls needed for most situations where information controls are used in industry and commerce."[370] Listing 11 control areas and more than 130 controls, it covers all aspects of organizational security, not just technology deployment. However, it imports a business model of information management designed to assess and manage risk with respect to the business organization. The privacy of individuals may be protected as an incident of protecting the business.

ISO27799 is an interpretation of ISO17799 for healthcare applications, and makes the protection of patient information very explicit. Yet it too is geared toward the data holders and application users rather than the patient. Privacy officers at health institutions can use such tools to avoid liability exposure and ensure compliance.[371] Generally, any cost function in the analysis is institutional cost – the dollar amount associated with a breach of privacy versus the dollar amount associated with implementing new provisions. The impact of non-compliance as analyzed is organizational, not personal.[372]

Privacy risk management is managed as an institutional threat. For example, Hong[373] defines its elements as: 1. likelihood of an unwanted disclosure 2. damage of disclosure and 3. cost of adequate privacy protection. Individual privacy may be protected as an incident of this analysis, but the main intent is institutional integrity.

There is plenty of interest in improving PIA process, with more emphasis on privacy issues and more focus on specific technologies. PIAs are recognized as too weak in technology evaluation.

"A lot of people are relying on privacy impact assessments and threat risk assessments then they are done their risk assessments. I think we need to go further, from a privacy policy perspective we need to look at the who, what, when, where and how in all cycles of that development whether it is business product development, policy development or technology development life cycle. Just always making sure that, yes you see identified that there's an issue here's how we can deal with it and then deal with it. We seem to sometimes jump right into building or buying something… You can't just do a PIA or TRA and think you're done with it, we need plans for continually updating those

[370] Fraser, R. (2006) "ISO 27799: Security Management in Health Using ISO/IEC 17799." Presented at *the Canadian Institute for Health Information Starring Standards HL7 Canada and Partnership Joint Conference*. Available online: http://secure.cihi.ca/cihiweb/en/downloads/Ross_Fraser_-_ISO_27799.pdf.

[371] Heckle, R. and Holden, S. (2006) "Analytical Tools for Privacy Risks: Assessing Efficacy on Vote Verification Technologies." Poster at the *Symposium On Usable Privacy and Security*. Available online: http://cups.cs.cmu.edu/soups/2006/posters/heckle-poster_abstract.pdf.

[372] Heck, S. (2006) "Privacy Enhancing Technologies: A Microsoft Perspective." Presented at *Electronic Health Information & Privacy Conference*. Available online: http://www.ocri.ca/ehip/presentations.html.

[373] Hong, J., Ng, J., Lederer, S., and Landay, J. (2004) "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems." In *Proceedings of the Designing Interactive Systems Conference*. 91-100.

assessments and policies. We need to be a little bit more proactive rather than relying on a bunch of audit trails in the long run "

While some commentators advocate risk management over legalistic compliance,[374] and insist it must form part of the technology design from project inception, this still does not address the focus on organizational, rather than personal privacy outcomes. "Compliance is [ideally] both to PHIPA and patient values and expectations."[375]

2.3.2 Public trust and confidence

Education and communication appear to be a priority among administrators. While public awareness around privacy issues is increasing, more public education is needed and occurring as acceptability to the public is seen as a key to successful system deployment.

"Telling people what to do shouldn't be a burden and it shouldn't be daunting. Telling them what you're doing with their information seems to be a real issue for a number of people in the health care sector."

As with other stakeholders, there is a belief that people think more sharing is occurring than really happens – that there is a public fear that is greater than with a paper system. People fear that their information is more easily accessed, while thinking nothing of the privacy issues involved in the paper system and how easily information might be mismanaged. Such "inaccurate" perceptions are seen as creating a barrier to research, health surveillance and other beneficial uses of data.

The cross-jurisdiction issues raise problems in administration as well. Nova Scotia and more recently, British Columbia have raised introduced legal provisions on cross-boarder movement of health information specifically with respect to exposure to U.S homeland security. This creates significant problems in directing technology deployment and use, when, for example, there is software development occurring in the U.S, or data housed in the U.S. Just to undertake the development of the software involves de-identification of information and intersection of rules and regulations.

Health information is recognized as more sensitive than other information leading to greater concern in the public mind over unauthorized use. The sensitivity of the information is tied to a higher concerns over confidentiality, and concerns regarding misuse of the data. Almost universally the concern is unauthorized access: "With regards to health information privacy there are things that should never be accessed even though you CAN access them. It becomes a privacy issue when those things are breached."

[374] "Privacy planning is more effective if approached from a risk management perspective than a legal compliance perspective", from Gurski, M. (2006) "Building Privacy and Security Technology into Health Care Environments. The Preconditions & Solutions." Presented at *Electronic Health Information & Privacy Conference*. Available online: http://www.ocri.ca/ehip/presentations.html.

[375] see footnote 374.

Confidence arises with the assurance that you have control that your info is not being shared outside of any situation you did not authorize.

3 Technology Developers

Most health care institutions turn to the vendor market for provision of its software, whether it is EMRs or EHRs or something more specific. In some jurisdictions, a variety of certification authorities will indicate whether the vendor product is compliant with jurisdictional requirements, security standards, and similar requirements. In addition to meeting such standards, the vendors respond to the requirements set forth by the health care entity/consumer which are their clients – those purchasing the technology solutions – often developed in risk assessment instruments or PIAs. If the jurisdiction has no central agency developing specific standards, the entity deploying the technology is responsible for its own compliance assurance.

Perhaps the most aggressive jurisdiction with regards to uniform compliance testing is Alberta. Alberta Netcare is a umbrella organization that provides a single identity for all activities and projects relating to Alberta's EHR system. While they do not themselves function as an oversight body,[376] they do provide a single point of reference for the concept of a provincial wide EHR, and produce and provide the Vendor Conformance and Usability Requirements (VCUR) to other agencies to test software compliance and standards. For example, VCUR is applied to EMR systems in Alberta clinics under the Physician Office Systems Program (POSP) [377]

The POSP is an is an initiative under the Master Agreement between the Alberta Medical Association, Alberta Health and Wellness– which oversees Netcare - and Alberta's Regional Health Authorities. POSP provides a standardized set of procedures and policies for the implementation of EMR systems.[378] The POSP maintains a list of vendors and products tested to conform with the VCUR, and thus available for integration under the Netcare strategy.[379]

The VCUR tests[380] therefore give a clear picture of minimum features supported by the 14 approved products. Included are role based access control (with six roles specified) with data masking, basic user authentication, recording of legislative authority to collect, use and disclose PHI, logging of PHI disclosures, basic encryption (passwords and remote access), and malware detection. This provides a snapshot reflecting the current level of expectations for technology deployment, compared to possible technologies discussed in Part I of this project.

[376] http://www.albertanetcare.ca/2.htm
[377] http://www.posp.ab.ca/vendors/VCURConformanceTesting.asp
[378] http://www.posp.ab.ca/about/
[379] http://www.posp.ab.ca/vendors/
[380] http://www.posp.ab.ca/vendors/VCURConformanceTesting.asp, as "VCUR 2006 Sections 7 and Section 8 Final Realease"

3.1 The Meaning of Privacy

The technology developers generally focus on data protection: "privacy to me means protecting that information." [n] Autonomy may be mentioned in the context of controlling and enforcing limits on access to people's information.[v,m] There are some variations on the theme, linking privacy to confidence in the system,[a] or awareness of the location of information,[h] or the ability to control the information.[w] One proffered view hilights the data protection versus autonomy distinction: privacy could be viewed as security applied to the individual's data when it was transmitted, but once data arrives some where (such as a server), the issue becoming data security.[w]

3.2 Technology Deployment Matters

The interview participants made much of the physical security and the human element in technology safeguards. "The problem with security is that it is a weakest link in the chain endeavor." [m] It is mistakes that cause breaches, usually mistakes among users: "it's physicians or someone making a mistake with an Electronic Record just because they did not know any better." [h] Lack of awareness or lax procedures contribute to the problem. [m]

The increased risks trace back to the recognized need to share information in health care. Physically, individual records are more secure from prying eyes, but there is recognition that networking and sharing of information has introduced another form of insecurity. "So in most ways an EHR is more safe than a paper chart. The problem is that if you have a security problem, you can have access to a lot of files. The bar is higher to get in, but if they succeed it is a bigger problem than with paper records (much more information has been compromised)."

This is the crux of the BFHD problem. Not only are large data collections more attractive for malicious intruders, but any anonymized data is easier to re-identify in the context of additional information. While there is explicit acknowledgment that large data sets import privacy risks, centralized registries encourage aggregation and provincial and local initiatives tend to support large aggregation of PHI into data repositories . Most vendors encourage the use of centralized databases (or at least a centralized service), as it improves their market position and scale of operations, as well as being the technology that is mature and proven.

This is only one aspect of technology evolving from business imperatives.[381]

Common privacy and security technology in vendor EMRs include authentication, user authorization, role-based access control and audit trail logging to monitor breaches.[382] Access control, where it exists, is most popularly RBAC. In general, vendors respond to particular requirements of particular clients, proffering a suite of possible solutions. [m] It

[381] Briney, A. and Prince, F. (2003) "Security Survey: Disciplined Security." Information Security. Available online: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss143_art294,00.html.

[382] This can be observed from vendor websites, *e.g.*, Med Access Inc. (http://www.med-access.net/pconf.htm) and JonokeMed (http://www.jonoke.com/jonokemed/security/index.htm).

is also remarked that uptake in health care is relatively slow. [h] However, there is ubiquitous use of encryption and logging technologies, [n, a, v] and always some form of authentication, although often this at times is little more sophisticated than password management. Vendors generally will help their clients with conventional security protection using firewalls, encryption for storage and transmission and secure networking.

Generally, the capacity is available to protect particular records from being viewed,[n] or masking records from particular users,[h] is available at some level, so that consent management is often available in the limited form built on RBAC access control, which handles consent related to specific roles. There is little distinction made between access control and consent management.

Separation of PHI and identifying information is advocated an important safeguard – a similar notion as encouraged in the separate registry and service components of Infoway's PSA architecture. (see *The Choices of Canada Health Infoway* on page 46) However, the appearance of separate services, some of which appear to duplicate functionality (authentication, authorization, federated identity management and so on) can also increase the points of attack on the system.

3.3 The relationship between policy and technology

Generally, all the technology implementation experts felt policy was responding positively to new technologies. Most thought that policy should not be technology specific, "if policy is well written then technology advances should not effect it, technology is changing continually, practically on a daily basis…Policy however should not change on such a basis." [m] Instead, procedures and operational decisions could deal with such changes. Policy goals themselves, however, should be technology-neutral.

There was also some support for the notion of incremental development of policy and technology – as technology outstrips policy, there should be more development [v] or that policy need to be informed by technology advances, [m] and some real confidence this was indeed happening.[a] "I am seeing the change provincially, and in some cases regionally. There are some really progressive governments out there that are producing some impressive policy recommendations" [h]

A popular view is that clear interpretation of existing policy is needed, rather than new policy [m] or more deliberate enforcement of existing policy. [v] These would speak to specific application of controls and how information would be handled and secured in specific technical terms. Others might characterize this as a need for "clearer policies" [w] speaking to specific technologies.

But there are dissenting views. These come from skepticism that policy makers genuinely understand the implications of the technology, how it can be used to identify you, and the implications of replacing the trust involved in talking to a human about your health with computer technology. "Mind shifts take at least a generation, and the technology has gone through many generations in one human generation" [w]

No doubt much of the difficulty stems from the complexity of consent and access concerns in health care: "The classic remedies that are applied in other industrial areas to information security problems, such as the separation of public and operational areas, are not effective in health care" [m]

3.3.1 Public trust and confidence

While the reception of these systems is generally cast as positive, data protection is seen to be a top priority among patients. There is some concern about the public being under-informed with respect to EHRs. "I don't think people have quite wrapped their heads around the potential implications of electronic health records" They may not understand how many people get access to files and how much easier that comes with electronic records compared to paper records. [v] The connection between privacy technologies and risk from breaches may be distorted by media coverage. [i, v]

There is general concern that the changing risk profile may not be understood by physicians either.[n] In general, physicians are characterized as reluctant to pay for security without explanation of their liability exposure and some support for their costs. [aa]

Vendors see physicians, not the public, as the client: "there is a requirement on the physician to educate the patient on what is going on…The physician must be comfortable with the system" [a] Their acceptance depends at least in part on convenience and usefulness of the system [i] This means that access limitations to health care professionals is a critical element of the implementation. RBAC or consent management that doesn't work well from the physician's perspective is a problem.

At the same time, it is understood that the system is subject to public acceptance. "The public would expect that the information on them in a medical emergency was available if that information was available in electronic form. Yet at the same time the public, and rightfully so, expect that the information be kept confidential and not shared with anyone who did not need have a need to know it". [m] This is not viewed as a simple technological feat: "Information flows to those who need to see it but it is difficult to determine who those people are in a previously arranged or fixed way" [m]

4 Primary Care

4.1 The meaning of privacy

> "Don't ever assume that anything is private. Nothing is private anymore!" [gg]

Doctors who are patient centric tend to adopt the informational autonomy notion of privacy, and focus on the ability of a patient to control information sharing, the sharing of personal information with other people. "Control should be completely with the patient to determine who will view the information." [g]

There is a view that personal information has a different texture when it was needed for health care – that informational autonomy is a privilege not a right in this context. "Clinicians and scientists today behave as if they have right to acquire patient data." [383] Health care providers expect to have access to their patient's information for the purposes of treatment. In fact, it is a tenant of good medical practice that the physician acquire the best information they can – sometimes with some reluctance on the part of the patient.

Data protection is seen as related – where privacy is about preventing access, [i] technology is seen as the tool that supports controlled access. [k] In other words, security technology is the means of implementing privacy. [p]

Privacy is something that is very personal in the doctor's perspective,[p] leading immediately to the notion of confidentiality. "People are a lot more emotional about their healthcare privacy and their personal lives, and they are a lot more likely to have to share intimate personal details during health examinations. Details they wouldn't share with their bank manager." [g] And this confidence pervades the data in multiple ways – even data in obscure computer codes (such as ICD-10 codes for procedures on a medical bill) can reveal very specific information regarding psychological, sexual diseases, and so on.[i]

For the physician, the real issue is the intent and ethical behaviour of the person accessing and using the data. If confidence and trust is observed, then there is no issue. But there is limited capacity for the physician to monitor this in an electronic system – it must be audited by the system, the patient or others.[p] Thus, the locus of confidence is altered, and the concern remains that there are people involved who don't understand or respect the nature of the confidence.[k] "…there could be deliberate browsing and inappropriate access by healthcare providers and other providers... There's also the use of the information once its collected, so secondary and teritary uses by a number of different entities, such as government, professional associations, and/or third parties such as drug companies who would love to get their hands on information to improve their corporate share." [g]

4.2 Technology Deployment Matters

The tension between improved data sharing and loss of control is well understood [p], as well as the dangers of increased data aggregation and linking for potential privacy breaches. [p, gg]

For the physician, technology choice revolves around how much value is added to their practice. A tool should improve patient care if properly utilized with security and privacy concerns respected [p]. The approach is ".. we are not going to serve the technology, the technology is going to serve us, and how is that going to do it? "[g]

Utilities like an upload/download capacity to transfer information between a chart and a pharmacy network are seen as valuable.[k] However, role-based access control may seem irrelevant to a physician who feels they are being handcuffed to share information only with prescribed individuals. For example, in a clinic with 17 thousand patients there has

[383] see footnote 364.

only been one request to restrict access.[k] Doctors claim that patients want others inside the clinic to be able to see the chart, [gg] and so access control becomes not a matter of improved patient care but rather a necessity introduced by the wider scope of EHR operation exposing the data outside the clinic.

Reservation has also been expressed about the effectiveness of consent management, particularly under a patient-centric approach. Experiences with earlier systems requiring cumbersome data entry or multiple passwords create poor expectations. [384] While identity management is intended as a response to this problem, it is unlikely that this relatively new technology will reach significant levels of penetration in the near future. A more likely response is a common service provider for most services, exacerbating the risk of data aggregation.

Difficulties around workflow disruption are also perceived to be a future barrier as well. Consent management is one explicitly mentioned: there is a concern that the complex requirements for consent and restrictions on implied consent could introduce unmanageable administrative overhead.[g] The same could as easily be said about complaint procedures, auditing and other requirements: the implementation of these requirements and their technological appearance simply hasn't been worked out.

Communication between systems is also problematic – as policies between hospitals or institutions differ.[385] PRM and similar technologies are meant to address these problems, but are currently not mature enough for widespread deployment. Sometimes the issue is as simple as reasonable access. If the user has to circumvent the access control mechanism to care for their patient, trust in the system is compromised as the technology either hinders or appears to hinder health care.

4.3 The relationship between policy and technology

There is strong consensus that privacy policy should guide "whatever the technology is able to do, or should be required to do" [k]. "There has to be very explicit policy before data is amassed, on what use it is going to be put to, who will access it, and who gets to say who has access. There needs to be a clear understanding of who controls access or the masking of the information. With that policy in place, the data can be collected." [g]

With so many factors to think about ahead of time, EMR projects have been known to fail without clear and deliberate planning.

At the same time, policy will have to reflect an understanding of technology at the time it is developed and try to match known technology to policy principles. [gg]

Some are cautious about the political drivers behind e-Health initiatives "There are going to have to be watchdog parties to see that principles are adhered to. Those within the system will have a vested interest in making this move ahead, but it may be at a price that

[384] see footnote 366.
[385] see footnote 366.

is unacceptable to somebody else." [gg] There are bureaucratic and public accountability pressures.[p] Both technological and social factors are involved and success depends on integration of both.

For the physician the problem may be the transparency of policy, or an understanding of how it will impact the health care provider in the context of their practice. One small town GP has been running his own privately built EMR for years. He has dealt with all the system issues of physical security, failed backups, compliance problems. Isolated from the internet, his EMR is distinctly non-interoperable and safe from hacking. His concern with EHR initiatives is not technology competence, but making sure the correct policy is in place and that it is transparent: "If the policy is not done right, potential [exists] for breaches of confidentiality, and a huge backlash when it happens…. Unless they have something in mind they haven't told us. I've read all the stuff they've made public on it, and I actually work with a guy who is on the committee. He means well, but I keep telling him they need to make their policy more apparent, and start selling it or its going to fail." [c]

In fact, doctors aren't worried about massive intrusion or large breaches. Like other stakeholders, they view the sloppy use or accidental release as more likely threats, [k, p, gg] but with an added focus on the requisite loss of trust.

The large scale breach is not discounted entirely,[386] and again there is a focus not around breach of privacy but the failure of public trust: "The reaction when people do it by accident is so overwhelming, if anybody did it on purpose…" [gg]

For the most part, doctors don't report patients being concerned about the technology [c] until it comes to the patient's attention that their own health information might become public. [i]

Most report positive responses by their patients to EMR introduction [p], with a mix of opinions on whether patients are cautious about the data is stored: patients in one practice inquired [gg] and weren't interested in another. [p]

Except for the extreme patient-centric practitioner, primary care providers do not involve the patient in the management of their health care information [s] and have a general reluctance for patients to have ongoing access to modify charts [dd] As with the legislation, there is no concept of a comprehensive PHR integrated into the system.

4.3.1 Public trust and confidence

The physician, as our example of the primary care provider, view patient confidentiality, not privacy, as the central tenant of the doctor-patient relationship. In our traditional health regime, the physician has longstanding traditional professional and legal duties to protect the confidentiality of their patients. The advent of privacy law adds a new

[386] One interviewee (c) has physically isolated his EMR from the internet for exactly this reason, and connects his data to the hospital by manually transferring it onto a flashdrive.

complexion to their obligations which has confused the matter. It is unclear to what extent the new privacy laws or health information acts have displaced the traditional obligations and it makes perfect sense for physicians to simply wait until such questions are answered before adjusting practice.

In the meantime, the physician is asked to entrust their patient's confidence to operation of an EMR. In an institutional context this is not hard to imagine; hospital records have always been controlled by the institution. What is different is the private physician trusting their private clinical records to a service provider, or even a provincially certified data service. If the physician's experience with the system has been less than congenial, there is little chance of engendering the requisite trust.

The doctor generally has a very clear and detailed view of how to construe implied consent, its relationship to trust, and how far it extends:

> I'm used to functioning in a world of implied consent. When patients come in the door to the office, there is an implicit understanding that they are there to seek some sort of advice about their health, and they are consenting to me doing what I need to do to give them that advice. Any time that I do something that is unusual or invasive or potentially harmful to the patient, the consent from the patient becomes more explicit. Sometimes is written. Any time I'm going to use their information for anything other than direct care, I'm under an obligation to make a very explicit disclosure and obtain from them explicit consent. So if I'm going to give information about them to a third party for some reason, whether for their benefit or research or whatever, I'm under an obligation get explicit consent. And I think the same applies in the electronic world. If I'm going to share information with a consultant, the method by which I do that is not relevant to the discussion; the point is that I'm sharing information so the patient is being given care. If I do it in a letter, fax, or email as long as I'm sure that whatever method transmission of that information is reasonably secure there's the implied consent for me to share the information. If I'm putting that information up on some sort public website, that's a totally different level of risk to the patient and a totally different consent that needs to occur. – ***Anne Doig*** [k]

Part of this perception is that patients expect the doctor to share the information in appropriate circumstances; it would be odd for the doctor to request explicit consent for such things as consultation with a specialist. Furthermore, patients are portrayed as having some sense and expectations of how this sharing functions in a conventional practice.[p] They trust their doctor to release highly sensitive information to the right people at the right time, not to exercise their own judgment as might be required in the new legislative and consent management regime. Survey results do suggest that government and managed health care are not trusted, and neither are "trusted" third parties that may be imposed by technologies.[387] Clearly, a mismatch between such operational notions of consent, sharing and the actual technology or legislative regime represents a shift in the norms of practice.

[387] Smit, M., McAllister, M., and Slonim, J. (2005) "Electronic Health Records: Public Opinion and Practicalities." In *Proceedings of the Networking and Electronic Commerce Research Conference*.

Physicians thus characterize themselves as gatekeepers for the information, and are reluctant to hand this function over to the technology or the legislation:

> When we told them that there data was upstairs on a server and it was actually safer there than when it was on a sheet of paper in our filing cabinets, they were noticeably pleased with that. They **liked** that! What they want is a gatekeeper in many respects. And it's that relationship that they have with their physician, and particularly a family physician, is that they look upon someone who has to be the primary caregiver, who has responsibility. That person will be the gatekeeper …. So when I make a referral, nobody ever says to me "What are you going to tell him?" They respect my judgment in terms of what I'm going to do in that respect. So … I cringe, at the challenge it would be if we suddenly had a check list of "you can share this, but you can't share that. You can share this under these circumstances, but not those. …. Now whether that's satisfactory as we get into increasing complexities of care and care teams, I think were going to be finding out and there's probably going to be some blips and bumps before we do.
>
> - ***Clayne Steed*** [gg]

5 Conclusion

Informational autonomy is the most cited definition of privacy, but a recurring concern recapitulates the observation from Part II of the report that there is more to privacy than informational autonomy. Personal dignity, confidentiality, trust and data protection are seen as concepts that reinforce and are related to each other in a different ways. Data protection is sometimes mentioned as supporting these other precepts, and at other times as inadequate engagement of privacy or the other concepts of dignity and confidentiality.

The concept of confidence and confidentiality was repeatedly raised. For the health care provider this is a central tenant of health care relationship: privacy may or may not be a result of the ethical and professional conduct of the profession. The notion of privacy is secondary to confidentiality and trust for the physician, or might possibly be portrayed as one *result* of confidentiality. With training, professional obligations and long held traditions in confidential handling of patient information, they express forthright and specific opinions on the nature, extent, obligations and relationships affecting the confidential exchange of information. Notions like intent and ethical behaviour are raised by this group of stakeholders, which do not appear in Part I or II or the report, and do not seem to significantly influence either technology design or the legislation surrounding data protection, other than the use of related words such as "custodian".

Part II of the report developed the distinction between data protection and privacy. One offering[388] introduces confidentiality as a third category, both conceptually and legally distinct. *Confidentiality* involves others in protecting information you have shared, whereas *privacy* relates information under direct personal control, each of which is distinct from legislation governing *data protection*.

[388] see footnote 357

Those in oversight and policy administration roles do not tend to engage confidentiality as a distinct problem. It is either integrated with privacy, or supports the basic privacy elements of personal dignity and integrity, through the mechanism of custodial data protection. This is not surprising, as the legislative mandate for oversight and policy administration under the current regime is about data protection. In other words, to accept that privacy and confidentiality have significant extension *other than* data protection would probably place it beyond their legislative reach, since the rules, procedures and legislation are about data protection. As noted in Part I of this report, the current technology embedded in the business-perimeter model reinforces this approach, as well as bringing the technology experts to much the same mindset.

All stakeholders recognize the balance between sharing data to provide the best care possible and protecting the PHI (whether as a privacy or confidentiality issue). The difference is that physicians view the technology and legislation as incidental or possibly as tools that might help achieve this balance, whereas other stakeholders seem to view them as an articulation of policy regarding the correct balance. The difference is a pragmatic one: technology or legislation that interfere (or are perceived likely to interfere) with those professional imperatives, particularly the best possible care of the patient, are likely to be treated with skepticism and/or circumvented by the health care providers. For others, they create the procedural framework within which the balance is to be achieved.

There is common agreement that most privacy problems are due to people. Most breaches are perceived to be inappropriate internal access or failure of an institution to enforce appropriate access control standards. Exposure to intrusion by outside "hackers" is often portrayed as a fear that is large in the public eye and media, but less of a real threat. The systemic concern is such a breach would result in a failure of public trust, with little idea of how to deal with the resulting public backlash. The more familiar, internal slips or inappropriate browsing by those inside the "circle of care" can be dealt with through institutional responses, which correct the infrastructure problem. The question of whether these really address the impact of the breach on the individual is seldom raised.

This distinction is very clear among some policy administrators, who will even separate technology purposes and role responsibilities based on this distinction: external intrusion is a *security* matter; inappropriate access by those in the circle of care or with access is a *privacy* matter. This shows a business-perimeter bias towards interpreting the technology and institutional process into question – suggesting the rules, processes and responses are about protecting the institutions and the system, which may incidentally protect the individual's privacy or confidentiality.

Concerns about specific technologies did not play a significant role in the responses. Some concerns were raised around the BFHD risk of aggregating data and thus creating attractive targets for intruders, and the maturity of certain security and privacy technologies was discussed, and the concept of role-based access control was raised. But generally, there was no concern with the potential for technology to function as it purports. More concern was raised whether the deployment of so much restrictive

technology was appropriate: in terms of shifting responsibility and trust away from the health care provider and onto the technology, in terms of hampering the delivery of health care, and in terms of whether there is any really meaningful patient control offered through consent mechanisms (both legislative and technological) that are available. The one technology singled out providing new privacy capability unavailable in the paper environment was the simplest surveillance technology: audit logs.

There was a wide range of views concerning the relationship between privacy and technology, and the question of whether technology is inappropriately leading policy development. One approach espoused that policy should articulate fair information practices with the proper balance between privacy protection and information sharing appropriate to the health care sector, independent of any particular deployment of technology. On the other hand, many bemoaned a dearth of specific policy-directed advice on the appropriate security and privacy protections to deploy, or were skeptical regarding the applicability of the advice available. To make matters more confusing, sometimes both points of view were raised by the same individual.

It would be nice to discount this confusion as differences in jurisdictions, or the difference between high level legislative policy and its interpretation at the administrative or operational level. The fact is technology choices are made independently in different locations or different jurisdictions at the operational level. Furthermore, these decisions that are often relegated to operational choices have significant privacy implications, as discussed in parts I and II of this report. The idea that the impact of general principles espoused in legislation on privacy outcomes is greater than the impact of specific implementation choices is not tenable.

There is no doubt that policy needs to adapt to new technology, and respond to situations that cannot be predicted in advance of technology deployment, while serving basic principles at the same time. In this sense, technology and policy must advance together. This dictates caution where technology is adopted first, and policy has to catch up.

Traditional doctor-patient confidentiality and trust are transformed by the legislation and technology of the computerized health care system. Instead of trusting the physician to keep a confidence, the patient must now place their trust in the computerized security and privacy mechanisms which are increasingly out of the physician's hands. Likewise, the health care provider must trust their professional obligations to these same mechanisms. This trust may extend even further: to the policy administrators, IT maintenance and service personnel in charge of the technology. The very authentication and consent management schemes designed to give us confidence in the system, may be in fact sending a very different message – that those in the circle of care are no longer to be trusted to behave appropriately, but are to be monitored and controlled in their activities.

Appendix A: Interview Participants

Part III of this report combines material from multiple interviews with connective and explanatory commentary. Despite the authors' best efforts, there is always a possibility that the intent of a participant's contribution was not completely captured or that it was used in a context which they would not consider apropos. The participants listed here have not endorsed the substance of this report nor any of its conclusions. Special thanks are extended to these participants for their generosity in contributing their time and insight.

a. Charles Aram, Technical Operations Manager, Egton Medical Information Systems Inc. (EMIS), Edmonton, AB.
b. M. Maurice Boisvert, Directeur, Agence de santé et de services sociaux de la capitale nationale
c. John Bosomworth, General Practitioner, Princeton, BC.
d. Leroy Brower, Director of the Health Information Act, Office of the Information and Privacy Commissioner of Alberta
e. Mary Carlson, Director, Office of the Information and Privacy Commissioner of British Columbia.
f. Fred Carter, Senior Policy and Technology Advisor, Office of the Information and Privacy Commissioner of Ontario.
g. William Cavers, British Columbia Medical Association Representative, Physician Information Technology Office Steering Committee, Vancouver, BC.
h. Mike Checkley, Product Manager, Optimed Software Corporation, Kelowna, BC.
i. Richard Denton, Family Physician, Kirkland Lake, ON.
j. Gary Dickson, Commissioner, Office of the Saskatchewan Information and Privacy Commissioner.
k. Anne Doig, Chair, Saskatchewan Medical Association's Legislation Committee, Saskatoon, SK.
l. Landis Esposito, Chief Privacy Officer, Winnipeg Regional Health Authority, Winnipeg, Manitoba.
m. Ross Fraser, Senior Security Advisor, Canada Health Infoway.
n. Randy Gaebel, VP Operations, Med Access, Kelowna, BC.
o. Julia Gallo, Senior Policy Analyst, Ministry of Health and Long Term Care, Government of Ontario.
p. Marshal Godwin, Director, Primary Healthcare Research Unit, Faculty of Medicine, Memorial University of Newfoundland, St. John's, NL.
q. Debra Grant, Senior Health Privacy Specialist, Office of the Information and Privacy Commissioner of Ontario.
r. Nicole Hamikor, Data Research Policy Coordinator, Health Data Decision and Support Unit, Ministry of Health and Long Term Care, Government of Ontario.
s. Verle Harrop, Medical Informatics Specialist
t. Richard Hodgin, Director of Public Policy, Health Canada
u. Sandy Hounsell, Executive Director, Office of the Information and Privacy Commissioner of Newfoundland and Labrador.
v. Stephen Johnston, Senior Research and Policy Analyst, Office of the Privacy Commissioner of Canada.
w. Susan Landau, Distinguished Engineer, Sun Microsystems Laboratories, Burlington, MA.
x. Avner Levin, Coordinator of Law, Faculty of Business, Ryerson University, Toronto, ON.
y. Lucy MacDonald, Director of Privacy and Communications, Newfoundland and Labrador Centre for Health Information, St. John's, NL.
z. Karen Mbatika, Legal Counsel, Commission d'accès à l'information du Québec.

aa. Brent Mitchell, Marketing Manager, CLINICARE Corporation, Calgary, AB.
bb. Heather McLaren, Director, Manitoba Health, Government of Manitoba.
cc. Angela Power, Privacy Analyst, Newfoundland and Labrador Centre for Health Information, St. John's, NL.
dd. Joan Roch, Chief Privacy Officer, Canada Health Infoway.
ee. André Simard, Directeur de projet, Dossier de santé électronique interopérable (DSEi) du Québec.
ff. Patrice St-Gelais, Legal Counsel, Commission d'accès à l'information du Québec.
gg. Clayne Steed, Chair, Alberta Rural Physican Action Plan Board, Edmonton, AB.
hh. Dianna Surette, Utilization Manager, South West Health and Chair of Information Management Quality Team, Yarmouth, NS.
ii. Sherri Tiller Park, Privacy Coordinator, Western Health Care Corporation, Corner Brook, NL.
jj. Violet Van Hees, Policy Analyst, Department of Health and Social Services, Yukon Government.
kk. Doug Watt, Regional Sales, Nightingale Informatix Corporation.
ll. Christian Whalen, Legal Counsel, Office of the Ombudsman, Fredericton, NB.
mm. Margaret Ann Wilkinson, Professor, Faculty of Law, University of Western Ontario, London, ON.