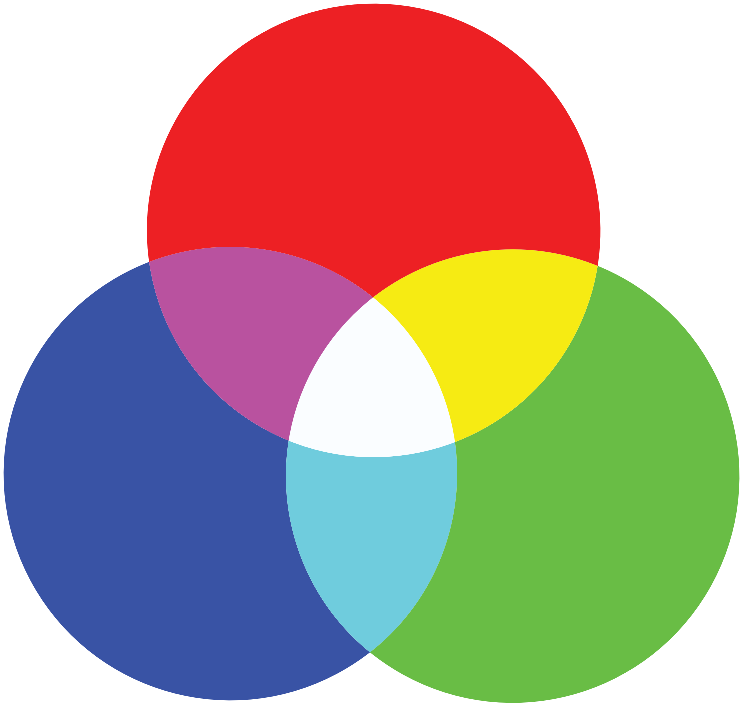
Encryption by Default
and
Circles of Trust

Strategies to Secure Personal Information in High-Availability Environments



December 2012

Sunnybrook
HEALTH SCIENCES CENTRE

Information and
Privacy Commissioner,
Ontario, Canada

CryptoMill

Acknowledgements

I gratefully acknowledge the contributions of: **Jeff Curtis**, MBA, MSc, CISSP, CISM, Chief Privacy Officer, Sunnybrook Health Sciences Centre; **Nandini Jolly**, President and Chief Executive Officer, CryptoMill Technologies Ltd and *Privacy by Design* (*PbD*) Ambassador; **Fred Carter**, Senior Policy and Technology Advisor, and **Michelle Chibba**, Director of Policy, Office of the Information and Privacy Commissioner of Ontario, Canada, in the preparation of this paper. I would also like to thank **Sam Marafioti**, Chief Information Officer, Sunnybrook Health Sciences Centre, for his leadership and support for this project.

Ann Cavoukian, Ph.D.
Commissioner

Information and Privacy Commissioner
Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

TABLE OF CONTENTS

Overview

This paper discusses the challenges of assuring strong security of sensitive personal health information (PHI) stored on portable storage media by organizations that require high data availability and use. The loss or theft of unencrypted mobile computing devices or storage media remains the No. 1 cause of breaches – 53 per cent of all U.S. health-care breaches reported since 2009.[1]

Encryption by default is the obvious solution. The power of the default cannot be over-estimated – the default rules! But encryption by default is not always easy to assure in large, complex health-care operating environments. Using the example of Sunnybrook Health Sciences Centre's leadership and policies, the paper illustrates how the *Privacy by Design* (*PbD*) Principle of "End-to-End Security" can be applied proactively and systematically, to become embedded in design and realize positive-sum results.

The paper also introduces the "Circle of Trust" concept, developed by CryptoMill Technologies. Modelled after the "Circle of Care" concept, Circles of Trust refer to mobile encryption deployment scenarios that enable the free flow of PHI strictly among authorized health-care providers, only for purposes of patient-care and treatment, while at the same time, ensuring that PHI remains encrypted and inaccessible to anyone else, by default.

This paper targets information management professionals and is intended to illustrate evolving security approaches and practices, with the help of two community partners: Sunnybrook Health Sciences Centre and CryptoMill Technologies. This paper explores the end-point encryption practices in place or being considered by Sunnybrook and provides an overview of emerging access control technology that can be applied within large-scale enterprise environments.

Together, we hope this paper stimulates discussion regarding the challenges and opportunities for ensuring the security of personal health information within health-care settings, and beyond.

[1] According to the official breach tally from the U.S. Department of Health and Human Services' Office for Civil Rights: http://1.usa.gov/a2UGEG

1.0 End-to-End Security

Data security is essential to information privacy. Indeed, without security, there can be no privacy. The *Privacy by Design* principle "End-to-End Security – ***Full Lifecycle Protection***" seeks the highest standard of data security possible.[2]

Personal data should be automatically and continuously protected, i.e., secure, during all stages of collection, use and disclosure, and during retention and destruction. Personal data should be protected by default (automatically) wherever and however it travels or resides – in a mobile device, in a corporate database, or in the Cloud – there should be no gaps in protection or accountability for secure storage or transmission. Thus, *PbD* ensures cradle-to-grave, secure lifecycle management of personal information, from end-to-end.

Assuring full lifecycle protection is a significant challenge for organizations today because their operations have become more data-intensive, more network-dependent, and more accessible than ever before. The explosion in the use of mobile devices such as laptops, smartphones, tablets, USB drives, and portable storage media, as well as the increasing use of personal mobile devices for business use, are causing a fundamental rethink of how best to protect the modern enterprise's sensitive data from "end-to-end."

As data processing technologies, business practices, and networked architectures become more complex and critical for operations, it is more important than ever to anticipate security risks as early as possible, and to mitigate those risks by building strong technical, administrative, and physical security practices right into the architecture and way of doing business, by default. The strength and convenience of security by default also supports *PbD* Principle #2: "Privacy as the ***Default Setting***."

The health-care sector is a particularly challenging area in which to deploy security controls for a number of reasons (discussed in the next section), but especially because of operational requirements for high availability and integrity of sensitive personal health information (PHI) used for patient care and treatment, research, and teaching purposes. In health-care settings, patients expect strong security and robust access control mechanisms to be in place. These expectations are supported by evolving legal and regulatory responsibilities governing the security of data handling practices, transparency of operations, and breach notification requirements.[3] A large, decentralized hospital complex, for example, will have special challenges to ensure end-to-end protection of sensitive data in an environment characterized by legacy systems, increasing interoperability, and 24/7 demands for access to accurate, up-to-date PHI for care purposes. These challenges are representative of an evolving landscape requiring both data availability and data protection on a large scale.[4]

[2] See full set of 7 *Privacy by Design* Foundational Principles at www.privacybydesign.ca

[3] For a discussion of health-care breach costs and incentives, see, *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced Security* (2012) at http://webstore.ansi.org/phi

[4] For a discussion of how applied privacy can strengthen organizational security, see Ann Cavoukian. (2005) *Identity Theft Revisited: Security is Not Enough*, at: http://bit.ly/eAuxg1 See also the following guidance on applying a "*Privacy by ReDesign*" approach to legacy systems: Cavoukian and Prosch, *Privacy by ReDesign: Building a Better Legacy*, at http://bit.ly/S2xT27 and Cavoukian and Popa, (2011) *Privacy by ReDesign: A Practical Framework for Implementation*, at: http://bit.ly/OMcuoW

2.0 Health-Care Security Challenges

As oversight authority for the *Personal Health Information Privacy Act, 2004* (*PHIPA*), the Office of the Information and Privacy Commissioner of Ontario, Canada (IPC) recognizes the challenges of providing strong privacy and security protection for PHI.

Large health-care institutions face security pressures due to the following:

- High demand for, and ease of accessibility to, personal data;
- Large numbers of authorized internal and, increasingly, external users who form the patient's Circle of Care;
- Increasing interoperability (and an associated increase in privacy and security) standards within regional shared systems and across provincial jurisdictions;
- Increased demand for and the need for rapid adoption of new information management technologies at the point of care (e.g. wireless networking, RFID, a ubiquitous electronic medical record) that do not in themselves provide secure sharing of information between users, devices, organizations, and government bodies;
- Increased complexity in the health-care IT support model due to all of the above, which results in an increased potential for technology configuration and management errors; and
- Increased strain on IT budgets and resources, including an increasing need for comprehensive security policy, procedures, and trained information security personnel, and especially including security-aware end-users.

2.1 Sunnybrook's End-to-End Security Challenge

Sunnybrook's information assets are, similar to all health-care institutions, vulnerable to loss or theft, facing a number of threats potentially affecting the confidentiality, integrity, or availability of these assets, including risks to the confidentiality of personal information and personal health information of staff, patients, and partners, and the privacy rights of the individuals affected by data loss. Insider and external threats leading to data loss or theft exist across all clinical and administrative activities involving data handling by Sunnybrook staff, partners, and patients.

Effective lifecycle management of data, therefore, requires a structured and standards-based approach to information risk management and should be composed of a core set of IT governance objectives addressing *data loss prevention*. Administrative (policy and procedure) and technical (logical and physical) security controls appropriate in these circumstances are required to reduce and manage risks to an acceptable level, which supports Sunnybrook's information management objectives. Data loss prevention controls ideally cover the complete range of corporate activities and threat scenarios associated with data collection, storage and use, data transfer, and disclosure (i.e. transfer within Sunnybrook and between Sunnybrook and its partners, peers, and patients), and data retention and destruction (and especially during the decommissioning of portable computing devices). Controls must address data at rest, data in motion, or data in use within each of these information lifecycle activity areas.

2.2 Encryption

Encryption technology and management are subsets of available security controls, which directly address the potential for confidential data loss or theft and should be applied to both data at rest (stored on media) and data in motion (during transmission over networks or during mobile device transport). For example, encryption controls should be applied during the transmission of data over otherwise unsecure networks (e.g. the Internet) by encrypting the data being transmitted and, ideally, by establishing a secure data transmission session between the sender and receiver. Data transmission security can be achieved by encrypting the data exchanged between the sender and receiver with or without securing the network connection or transmission session itself, with the parties either manually or automatically exchanging a decryption key using another secure channel (e.g. encrypting email before sending over the open Internet using a prearranged password or other decryption key).

Data at rest can be encrypted either at the file, folder, or whole disk level at the time the data is stored, and the data should remain encrypted until accessed by someone who possesses the authorization to access and decrypt the information. In practice, there is a need for balance between usability and security and encryption controls are no exception. In many institutional settings, for example, users may be able (conveniently) to use their system logon ID and password to act as the effective decryption key (or as credentials for automatic access to a separately stored key) when logging onto a personally assigned laptop. On the other hand, single factor (i.e. password only) logon schemes such as these typically employ a compensating lock-out feature if logon attempts exceed a preset threshold in order to (slightly) reduce the chance of unauthorized access attempts through password guessing. If logon is successful, the data remains accessible throughout the user session until the session is logged off or the laptop is shut down. In these common use scenarios, caution must be exercised by the user to ensure that the device is not lost during the logged on session where the data may be available to anyone with physical access to the device. Potential loss of data in this scenario can be further mitigated, therefore, by the use of an appropriate time out device (e.g. a password protected screen saver) which locks the device after a preset time of inactivity, and requires user authentication to re-establish the session and also gain access to otherwise encrypted data.

Encryption solutions (whether for data in motion or data at rest) can be applied either as an enterprise "end point protection" (EPP) or "data loss protection" (DLP) solution (e.g. as part of a centralized security policy enforcement suite, which may also include port and plug-in device control with auto-encryption options) or as a stand-alone end point solution applied on a case-by-case basis, possibly at the discretion of the data or system owner, one data set, device, or service at a time. Email encryption, for example, can be applied using either centralized, multi-institution services such as eHealth Ontario's ONE Mail service[5] (now available to most Ontario hospitals) or by engaging a commercial service provider for custom email encryption solutions, typically requiring each email recipient to register themselves with the service the first time they receive encrypted email. The usability and convenience to both the sender and the recipient in using this type of service is often a strong factor in the balancing of considerations for selection, deployment, and management of specific encryption solutions by an institution.

2.3 Mobile Device Encryption

Storage of data on an unencrypted mobile computing device such as a laptop, USB key or portable drive, or a smartphone presents an inherent vulnerability to physical loss or theft and so the data needs to be protected from inappropriate access, should the device itself go missing. The proliferation and the diversity of these devices (many of which are, increasingly, not corporately provisioned but are originally personal devices, and which continue to be used as personal devices at work) has also increased the need for comprehensive security of the data accessible on or through these devices.

When assessing the likelihood of data loss due to a lost or stolen mobile device, the key privacy compliance issue is that, without prior knowledge of or control over what data goes onto a device, a health information custodian cannot unfortunately, rely solely on the goodwill or discretion of the user as to what he or she stores on the device or to determine whether the device should be encrypted to protect confidential data. Users may be either unaware of the data actually stored on the device at the time of loss, or may simply underestimate the nature or extent of data actually at risk. Sunnybrook's default risk position is, therefore, to assume confidential data assets are, in fact, stored on each mobile device and therefore, each device must be encrypted in order to ensure that the risk of data loss is absolutely minimized should any device actually go missing. Deployment and support implications for such a comprehensive strategy entails that all portable devices used for Sunnybrook business purposes must be demonstrably encrypted at all times, whether they contain PHI or not.

The diversity of mobile devices, which are increasingly personally provisioned for Sunnybrook's business purposes, the need for legal and policy compliance assurance, and the need to avoid disruption to the availability of, or loss of, non-recoverable Sunnybrook data, therefore means that mobile encryption is here

[5] www.ehealthontario.on.ca/en/services/one-mail

to stay, even if the provisioning of universally reliable, convenient, and secure remote access solutions becomes available for most use cases. Implementing a comprehensive but flexible mobile device encryption strategy across all possible use scenarios is the key theme of this paper.

2.4 An Overview of Sunnybrook's Mobile Encryption Strategy

There are a number of recognized best practices for identifying data at risk and for selecting appropriate mobile encryption controls to prevent data loss. Sunnybrook's Information Services group is actively involved in the following data loss risk management activities, which are expected to lower data loss exposure and contribute to a comprehensive data loss management strategy over time.

As a matter of best practice for data lifecycle risk management, Sunnybrook is fundamentally ensuring that it is following a systematic information security program for data loss protection across the lifecycle of collection, use, transmission/ disclosure, retention, and destruction, with a focus on appropriate encryption for data in motion and data at rest, where required. Mobile devices and laptops, in particular, are encrypted on first admission to Sunnybrook's network (even if presented as a personal device) or prior to deployment (if corporately provisioned) to ensure that the device is either adequately encrypted before use for Sunnybrook business purposes or is refused access to the corporate network or other corporate computing services. Encryption is thereafter monitored as part of a comprehensive set of device compliance checks including, for example, corporate policy based anti-virus management.

To accomplish a risk-managed approach for data loss protection, and particularly for the risk-based selection of encryption policy, procedure and technology controls, Sunnybrook is following best practices for identifying data and devices at risk and implementing controls that are appropriate for the associated risk profile and for management's corresponding risk tolerance and appetite.

These practices include:

1. **Determining what data is most sensitive and where it resides.** Sunnybrook is completing a data asset discovery, classification, and inventory which identifies and prioritizes data assets which are created within the enterprise, enter via network boundaries (e.g. via the Web, email or partner interface) or are physically transported via portable media (laptops, smartphones, USB devices). As a matter of best practice, identification of data in the institution's custody and control is always the first step towards accountability over potential theft or loss.

2. **Understanding the origin and nature of data loss risks.** Sunnybrook Information Services undertakes both privacy impact and security threat risk assessments of the most likely scenarios constituting loss of data assets and services, based on identified system, application, and database vulnerabilities, threat likelihood estimates and asset sensitivity and exposure.

These reviews are intended to reveal priority areas for risk remediation, and contribute directly to Sunnybrook's emerging IT Governance Program and overall information security posture.

3. **Selecting appropriate information management controls based on policy goals, risk objectives, and the location and use of sensitive data.** Health-care institutions, like any other data custodians, cannot afford to mitigate all data loss risks at once, and should, therefore, choose controls that are commensurate with the risk level presented, conditioned by management's risk tolerance (variability of outcome) and appetite (absolute loss aversion). From a legal compliance and ubiquity of use perspective, mobile device encryption (and the associated asset management and network security supports) represents a key area for continued Sunnybrook integration with enterprise security management policies, tools, and processes.

4. **Managing security centrally.** Sunnybrook continuously evaluates the deployment, usability, and support success of encryption technologies which are susceptible to the risk of policy misalignment, increasing management costs, and user complacency, over the lifecycle of the affected data assets, devices, and evolving user needs. Opportunities for increased integration of encryption technologies, key management across platforms and devices, and compliance monitoring and auditing are being constantly re-evaluated to take advantage of improvements in centralized asset and network access management, policy maturity improvements and orchestration, and improved platform, application and database hardening based on risk priority, where appropriate. The diversity of needs and devices, coupled with innovations in the core supporting technologies, means a move to increased end-point security flexibility with greater centralized visibility and control over data loss risk profile over time.

5. **Auditing security performance for constant improvement.** In conjunction with an emerging IT Governance program based on the COBIT[6] process control framework, Sunnybrook is improving its monitoring of security functions which support data loss prevention, including remote monitoring and management of encrypted devices, and is increasingly putting into place end-user accountabilities for the protection of data assets at all levels of system, application, device and database ownership. Formalized and consistent accountabilities for risk-based incident investigation, management reporting, correlation of security related incidents, and auditing and enforcement of data security policy compliance supports and strengthens data loss risk profile and is expected to result in greater compliance with privacy regulations and best practice standards over time.

[6] www.isaca.com/cobit

3.0 Using Technology for Better Risk Management

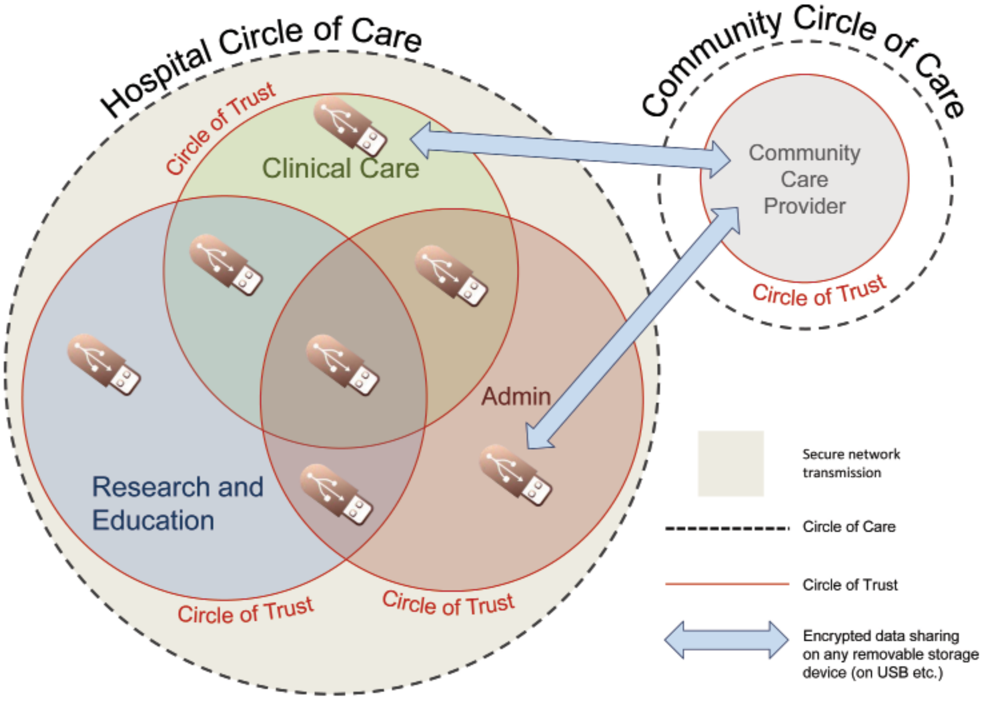
So far, we have described organization-wide policy and administrative options for securing PHI on mobile devices against loss or theft. Proactive leadership, expressed by systematic security methods, are consistent with *Privacy by Design's* emphasis on holistic, embedded, and verifiable approaches to privacy and security.

Regardless of how it is deployed in operation, mandating encryption by default goes a long way towards meeting the challenges of securing an organization's expanding perimeters, and for achieving compliance objectives.

There are, however, opportunities to improve upon the binary distinction between "inside" and "outside" an organization's security perimeter, and between all-or-nothing access to encrypted PHI. Innovative new approaches to securing PHI on mobile devices can enable new functionalities and benefits, such as enabling selective access controls to help protect PHI against the risk of unauthorized access by *insiders*.

3.1 CryptoMill Trust Boundaries and Circles of Trust

A Trust Boundary (TB) is a novel security mechanism introduced by CryptoMill Technologies that provides data containment by binding specified data to a defined group of users (generally, an organization or a subgroup therein). Using CryptoMill's *Zero Overhead Key Management* technology in conjunction with their *Intelligent Port Control*, organizations can prevent the decryption of sensitive data outside of the Trust Boundary. Since the protected data is strongly encrypted, it is completely inaccessible for any user outside of the defined Trust Boundary, but fully and readily accessible for those users within the TB.



Applying the Trust Boundary technology leads to the creation of a Circle of Trust. Circles of Trust become a means by which information stored on mobile devices is made readily available to authorized parties "inside the circle" (the *trusted parties*), while remaining protected from, and inaccessible to, external parties. Importantly, collection, use, and disclosure rules are formally defined for both internal and external parties as a whole, such that access rights need not be managed for each possible data recipient or potential information use case. The concept of a Circle of Trust shares commonalities with the Circle of Care concept, applicable within health care for the management of personal health information, and is, therefore, another means of enforcing access rights and improving data loss prevention within otherwise high availability environments.

3.2 Desirable Security Properties of Trust Boundaries

The Trust Boundaries concept offers the following desirable properties when applied to portable storage devices:

- **Data Protection through Intelligent Port Control:** In the context of encryption, port control ensures that any portable storage device plugged into a corporate workstation is first encrypted *prior to permitting data to be copied onto the device*. From a security perspective, this ensures that every portable storage device in use is encrypted, reducing or eliminating the security risks due to the transfer of data to an unencrypted mobile device. Intelligent Port Control ensures that the encryption is only applied to specified device types – an important deployment and support consideration in environments (such as Health Care) which continue to rely on USB connectivity for many devices other than portable storage.

- **Circles of Trust:** In contrast to stand-alone encryption schemes, which typically restrict the use of the encrypted device to a single individual, the Trust Boundary can be expanded to multiple users or groups who may need access to the information after it has been transferred to the portable media. This reduces the proliferation of portable storage devices, since devices can be shared and reused by members of the Circle with the membership able to be (re)defined dynamically and centrally managed.

- **Easy Group Sharing:** The automated encryption and decryption key management service allows for simple access to data by authorized individuals, without requiring passwords or otherwise increasing the accessing party's burden. As a matter of user-centered design, this improves the usability of the security feature and therefore directly supports *Privacy by Design* principles.

    - **Prevention of Internal Breaches:** Curious (or malicious) individuals outside of the Trust Boundary cannot access the data on the device, even if THAT person has the CryptoMill software installed and has access to other (different) Trust Boundaries within their organization. In this way, data cannot be removed from the Trust Boundary, as it cannot be decrypted on computers or by people outside of it. This feature is explained further in Section 4 below.[7]

This makes the Trust Boundary a **positive-sum solution,** in that it increases both data security (against unauthorized use or access) while increasing availability to authorized users. Further, it makes the Trust Boundary an intriguing platform upon which the Circle of Care can be technologically implemented.

3.3 The *PHIPA* Circle of Care

Under Ontario's *PHIPA*, it is recognized that in some cases the effective provision of health care will require sharing an individual's personal health information among multiple health information custodians (a family doctor, pharmacist, hospital, etc.) without the need to obtain the patient's express consent for each disclosure. To facilitate the transfer of PHI between health information custodians for the purpose of providing health care, the concept of the Circle of Care was developed.[8]

The act of sharing (disclosure) brings the new custodian into the Circle of Care. Thus, from an information security perspective, a Circle of Trust – a set of authorized entities implicitly assigned data collection, use, and disclosure rights – is created.

However, the means by which data remains accessible inside, but inaccessible outside, of the Circle of Trust remains undefined by the concept of Circle of Care. While this could be (and often is) implemented largely by policy and goodwill, from both a security and *Privacy by Design* perspective, it is preferable to build privacy protections into both the data technology and sharing practices of such a system.

Privacy by Design emphasizes that protections be built into information technologies, business practices, physical design, and networked infrastructure, by default. Creating a Circle of Trust is no exception. While it is possible to implement such a system based on acceptable usage policies alone, the true strength of the Circle of Trust is only seen when embedded technological protections operate in concert with usage policies.

[7] Simple device encryption (without Trust Boundaries) covers situations where the device is lost or stolen. These are scenarios where the new "owner" of the physical device is completely unrelated to the original organization. Simple device encryption covers the "mishap" case – one which conscientious people try to guard against (loss/theft) and is therefore an exceptional circumstance. With Trust Boundary protection, however, data loss is prevented in more common scenarios where access to devices is by people who have a right to be in the vicinity of the data, and who have rights to access data from other parts of the organization. USB storage devices borrowed by co-workers and other legitimate employees inside an organization are not typically considered to be lost or stolen. Yet, in these scenarios, it is easy for sensitive data to migrate into the wrong hands (intentionally, or accidentally). A third scenario, involving the need to access data on a protected USB drive from a foreign computer (for example, a presentation) would require a password-based solution.

[8] For a full discussion, see Ann Cavoukian. (2009) *Circle of Care: Sharing Personal Health Information for Health-Care Purposes*, at: http://bit.ly/R2Isep

4.0 Illustrative Deployment Scenarios

Taken collectively, the data protection features of "Intelligent Port Control" represent an innovative new positive-sum approach to solving the data in motion security concerns while enabling shared authorized access with removable storage devices. As noted above, this approach is distinctly different than traditional methods, which we refer to here as "Legacy Port Control."

1. Detection of Storage Devices versus other USB Devices

Intelligent Port Control specifically controls data storage devices, which include removable hard drives, USB flash drives, memory sticks, and other portable storage media. Unlike some Legacy Port Control systems, this is not an "all-or-nothing" option: Intelligent Port Control leaves all other USB devices alone. USB equipment (e.g. mice, printers, scanners, or specialty medical equipment) are not controlled, and operate without interference.

2. Automatic Device Management

Intelligent Port Control storage detection is automatic – if the inserted device looks like a "storage-to-Windows" device, it will be controlled. A given device is considered "storage," in this sense, if it implements a disk-like interface that presents a Windows-recognized block-oriented file system (such as FAT, FAT32, or NTFS). For such devices, Windows automatically mounts the file system, and the device's content is typically visible as files within Windows Explorer. Common examples of such storage devices abound, and include USB flash drives, removable USB, and FireWire (IEEE 1394) disks, SD cards, and memory sticks.

Unlike some Legacy Port Control systems, there is no need to maintain white and black lists of Device ID's, Vendor ID's, and Device Model ID's. Managing lists such as these is cumbersome, prone to error, security breaches, and annoying for end-users who have to wait for IT technicians to unblock their access to new removable media. It also eliminates the need for pre-encrypted or proprietary storage devices – any commonly-available, easily-purchasable device can be encrypted.

3. Can use both Encrypted and Non Encrypted Storage

Intelligent Port Control differentiates between encrypted storage and non-encrypted storage, applying different policies for each. The control policies are set by the organization, and can be user and user-class specific. Typical policy settings will allow full Read/Write access to encrypted storage, and Read-Only access to non-encrypted storage. In this way, information from outside of the organization can be brought in conveniently (if so desired), without requiring the introduced device to be encrypted, at the same time without the fear of "opening the gate," and letting sensitive data leak out to an unencrypted device.

Thus, one can have all the data management convenience and ease-of-access expected from using removable media, without the worry that data at rest (e.g. computer workstation-based information) can migrate out to an unencrypted mobile device.

4. Trust Boundary Technology Applied to Circles of Trust

Intelligent Port Control combines with CryptoMill's Trust Boundary technology in two different ways to increase the security and usability of removable storage devices:

a) *Secure Sharing via Password and Device Binding*

Users of a USB drive can institute a Sharing Password, known only to the members of the Circle of Trust (or, perhaps a small number of them), after which that device can be shared easily between those members. Each user can simply plug in the drive, enter the Sharing Password, and enjoy full use of the encrypted device. If the device gets into the wrong hands, the data cannot be accessed by anyone outside of the Circle of Trust, even if they come to know the sharing password, because decryption of the portable device is bound to a predetermined set of USB ports (typically designated corporate workstations or laptops).

b) *Secure Sharing via device Binding Only*

With this option, the Users of a USB drive can simply plug in the device and use it with no password to be entered at all. Similar to the Password Sharing solution above, if the device gets into the wrong hands, the data cannot be accessed by anyone outside of the Circle of Trust, since decryption of the portable device is bound to a predetermined set of USB ports.

5. Sharing Outside of an Established Circle of Trust

Sending a protected file to a trusted third party outside of an established Trust Circle is also straightforward: the file is selected for encryption, encrypted and then attached to an email or downloaded to an unencrypted USB drive. The recipient is separately provided with a password by the sending user. The recipient then uses the supplied password and a decryptor utility to access the encrypted file. CryptoMill offers a free File Decryptor that does not need to be installed and can run on a Windows computer by any user.

5.0 Conclusions

Privacy needs to keep pace with changes in technology, making security assurance increasingly difficult to achieve. As the environment, requirements, risks, and challenges evolve, so too must the methods of preventing data loss and theft. One of the single greatest challenges (and most obvious and growing risk) is the proliferation of portable end-point devices and storage media which are lost, stolen or compromised, in staggering numbers. While encryption of end-point devices is not a new technology, the need for seamless access in high availability environments means that deployment and support considerations are of prime consideration when considering optimal solutions.

Fortunately, these challenges can be successfully met by appropriate policies and innovative technological tools that are designed to ensure sensitive data such as personal health information is automatically encrypted by default, while at the same time, ensuring that the encryption process does not prevent the authorized use of the health information by those who enter and exit from a Circle of Trust, based on a rapidly changing service provision environment. Health care is one of those environments which is benefitting, and can benefit further, from improvements in security technologies which enable the delivery of privacy for patients, while enabling full access to information where and when, it is needed, without significant user or institutional burden. “Smart” encryption is one of the most important technologies that can and must be deployed in this fast changing sector.

Whether you are a large teaching hospital, a small clinic, a research facility, public service institution, or a private-sector contractor, the message is the same: secure your perimeter and end-points against unauthorized access – encrypt by default!

6.0 References

6.1 Selected Information Resources

IPC Orders relating to use of encryption on mobile devices under the *Personal Health Information Privacy Act (PHIPA):*

- Order HO-004 (March 2007) – Theft of a laptop containing the unencrypted PHI of 2,900 individuals;
- Order HO-007 (Jan 2010) – lost unencrypted USB memory stick containing the PHI of 83,000 individuals attending a flu clinic;
- Order HO-008 (June 2010) – hospital nurse has unencrypted laptop stolen from car;
- Special Investigation Report: (July 2012) – Investigation into the loss of two USB keys containing unencrypted personal information by Elections Ontario.

IPC Orders relating to unauthorized access to PHI under *PHIPA*:

- Order HO-010 (Dec 2010) – A patient's PHI held by a hospital was accessed by a technologist who was not providing care to the patient; and
- Order HO-002 (July 2006) – A patient's PHI was accessed by a nurse who was not providing care to the patient.

IPC Fact Sheets and Other Guidance:

- IPC Fact Sheet #12 – Encrypting Personal Health Information on Mobile Devices (May 2007);
- IPC Fact Sheet #16 – Health-Care Requirement for Strong Encryption (July 2010);
- IPC and Children's Hospital of Eastern Ontario, Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes (Sept 2011);

Other IPC Guidance and Discussion Papers

- Ann Cavoukian, The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices (May 2010);
- Ann Cavoukian, Identity Theft Revisited: Security is Not Enough (Sept 2005);
- IPC Fact Sheet #01 – Safeguarding Personal Health Information (Jan 2005);
- Safeguarding Privacy in a Mobile Workplace; Protect the information you keep on your laptops, cellphones and PDAs (June 2007); and
- IPC STOP. THINK. PROTECT campaign (ongoing)

Overview of Organizations

Office of the Information and Privacy Commissioner of Ontario (IPC)

The role of the Information and Privacy Commissioner of Ontario, Canada, is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The IPC acts independently of government to uphold and promote open government and the protection of personal privacy. Under the three *Acts*, the Information and Privacy Commissioner: resolves access to information appeals and complaints when government or health-care practitioners and organizations refuse to grant requests for access or correction; investigates complaints with respect to personal information held by government or health-care practitioners and organizations; conducts research into access and privacy issues; comments on proposed government legislation and programs; and educates the public about Ontario's access and privacy laws. More at: www.ipc.on.ca and www.privacybydesign.ca

Sunnybrook Health Sciences

Sunnybrook Health Sciences Centre is one of the largest hospitals in Canada. Its 10,000 staff, physicians and volunteers provide the best care for critical times in the lives of the one million patients it sees each year. Over the past 60 years, it has evolved from its original role as a veterans' hospital into a centre of excellence in patient care, education and research. Today, it specializes in caring for Canada's war veterans, high risk pregnancies, critically-ill newborns, adults and the elderly, and treating and preventing cancer, cardiovascular disease, neurological disorders, orthopaedic and arthritic conditions and traumatic injuries. Sunnybrook is fully affiliated with the University of Toronto, and provides learning opportunities for more than 2,000 students annually. Sunnybrook is also a research-intensive hospital. Each year, more than 600 scientists conduct $100 million in breakthrough research. Its commitment to excellence has resulted in an international reputation and a vital role in the Ontario health-care system. It offers highly specialized services unavailable in other communities. More at: www.sunnybrook.ca

CryptoMill Technologies

CryptoMill Technologies Ltd. is a Toronto-based company that provides innovative data security solutions for enterprises and small to medium businesses. CryptoMill also has offices in Barbados. It's advisory board includes experts in Health Care, Financial Institutions, and Technology. The management team is critically aware of the importance of security to privacy and embeds these principles into the design of its solutions. SEAhawk is a suite of software that provides advanced security, which helps organizations comply with data protection and accountability regulations including health information legislation such as PHIPA (Ontario), PIPEDA, HIPAA (US). Our solution protects data on laptops and desktops, and prevents data leakage through any removable storage device, including USBs, all from a single management console. It also provides comprehensive security capabilities for "data-at-rest" and "in motion" within an organization in a highly secure and easily deployable package. Organizations can choose either Basic Protection or Premium Protection. More at: www.cryptomill.com

**Office of the Information and Privacy Commissioner,
Ontario, Canada**

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

The information contained herein is subject to change without notice. Sunnybrook Health Sciences Centre, CryptoMill Technologies Ltd. and the IPC shall not be liable for technical or editorial errors or omissions contained herein.

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

December 2012

Information and
Privacy Commissioner,
Ontario, Canada