PRACTICE ADVICE

SAFEGUARDING PHI ON MOBILE DEVICES

DATE: 2010

SAFEGUARDING PERSONAL HEALTH INFORMATION ON MOBILE DEVICES

The following is an article on encryption of personal health information, which has garnered much attention in the last few years. It summarizes a recent order issued by the Information and Privacy Commissioner/Ontario; it outlines some of the risks and methods associated with dealing with personal health information on mobile devices.

CASLPO hopes that members are aware of the need to ensure the protection of personal health information on all electronic devices, and to discuss encryption needs with their employers.

SAFEGUARDING INFORMATION ON MOBILE DEVICES

In 2007, the Office of the Information and Privacy Commissioner of Ontario (IPC) issued an order directed to all Ontario health information custodians not to transport personal health information on laptops or other mobile computing devices unless the information was encrypted. This direction was included in a 2007 order under the *Personal Health Information Protection Act (PHIPA)*.

In December 2009, a USB key containing the health information of almost 84,000 patients who attended H1N1 flu vaccination clinics in the Durham Region was lost. This resulted in an investigation into the incident by the IPC, who deemed it a major privacy breach. The main issue related to the fact that the personal health information stored on the USB memory stick was not encrypted; had it been, this would have merely been the physical loss of a single USB key.

The Privacy Commissioner, Ann Cavoukian, was distressed by this incident in light of the order issued in 2007. "Some health information custodians are encrypting personal health information placed on mobile devices, while others are encrypting all health information", says Dr. Cavoukian. "But some custodians have not yet taken such necessary steps. Health information custodians **cannot** wait until they become a victim before taking concrete action to protect the personal health information, for which they are responsible".

As part of the order issued to the Durham Region following its investigation, Dr. Cavoukian included a message which is directed to **every health information custodian in Ontario**. The contents of this message are reprinted below.

COMMISSIONER'S MESSAGE

Ann Cavoukian, Ph.D.

Health information custodians in Ontario are required under the *Act* to take reasonable steps to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure. In 2007, following the loss of a laptop containing personal health information, I sent a clear message warning all custodians against storing personal health information on mobile devices, that are especially vulnerable to both loss and theft. In Order HO-004, I outlined a new standard to be followed – a multi-layered approach to guard against unauthorized access to personal health information stored on mobile devices.

It is always preferable to *avoid* storing any personally identifiable health information on mobile devices. However, where personal health information must be stored on such devices, the following measures are necessary:

- only the *minimal amount* of information necessary should be stored, and for the
- *minimal amount of time* necessary to complete the work;
- whenever possible, personal health information should be *de-identified* or *coded*, in a manner such that the identities of the individuals whose personal health information is stored on the device could not be readily ascertained if the information were accessed by unauthorized persons;
- if the information is coded, the code that is needed to unlock the identities of individuals should be stored separately on a secure computing device, such as a central server in a health care facility;
- the use of *strong password protection*; and, most important;
- the use of *strong encryption*.

The *Act* requires custodians to notify individuals if their personal health information is lost, stolen or accessed by unauthorized persons. Consequently, privacy breaches tend to be both time-consuming and costly, and often result in irreparable damage to a custodian's reputation and image. While I accept that custodians may not be able to totally eliminate the loss or theft of mobile devices, what I cannot accept is that the information contained therein is not encrypted. Unauthorized access to health information stored on these devices that happen to be lost or stolen may clearly be prevented through the use of encryption technology. However, despite strong incentives to avoid privacy breaches and the availability of encryption to prevent such breaches, unencrypted mobile devices continued to be used. This is both distressing and completely unacceptable.

Multiple factors may contribute to the failure to adequately safeguard personal information. First, there may be a lack of understanding about the vulnerabilities, threats and risks to the information stored on mobile devices, or a lack of awareness about what constitutes reasonable safeguards for personal health information stored on such devices. Second, there may be challenges in implementing enterprise-wide solutions that allow custodians to effectively manage and control the manner in which all of their agents and electronic service providers collect, use, disclose, retain, transfer and dispose of personal health information on their behalf. Third, while this is difficult to believe, some custodians may have interpreted Order HO-004 narrowly as applying only to mobile computing devices such as laptops and personal digital assistants, without recognizing that other portable data storage devices, such as USB memory sticks, pose similar risks. The stolen laptop that resulted in HO-004

and the lost USB memory stick resulting

in the current Order are instances of a growing class of security and privacy problems, namely data leakage and data loss associated with all portable storage devices. My office is taking steps to ensure that all of these issues are addressed.

As the health sector moves towards electronic health records and electronic systems of personal health information, public confidence in custodians' ability to protect all types of health records is essential. Privacy breaches stemming from the use of technology, without the necessary privacy and security safeguards such as encryption, will inevitably be viewed as harbingers of the state of privacy once the health sector makes the transition to electronic health information. In my view, this is completely understandable. After all, if custodians cannot be trusted to protect the personal health information stored on a simple portable device such as a USB key, how will they ever manage to protect the massive amounts of personal health information that will eventually reside within complex systems of interoperable electronic health records?

It is vital that custodians recognize that any breaches stemming from the improper implementation of information technologies will not only be costly for the responsible custodian, but will also reinforce skepticism about the health sector's ability to protect privacy in context of ehealth, in general. Increased skepticism will likely have a chilling effect on the acceptance and adoption of all types of new health information technology, including electronic health records. Given recent setbacks in the ehealth agenda in Ontario, additional barriers or delays are the last thing the health sector needs at this point in time. Therefore, it is essential that all custodians demonstrate both their commitment and their capacity to protect personal health information stored in all formats, now. Otherwise, the transition to the use of electronic health records will be far from smooth.

In recognizing the broader implications of large scale breaches of health information and the need to ensure that immediate steps are taken to prevent avoidable breaches involving mobile devices, I approached the Ministry of Health and Long-Term Care. They have committed to work together with my office to develop a communications strategy to help ensure that the entire health care sector in Ontario adopts reasonable safeguards to protect personal health information stored on all types of electronic devices. As a first step in this strategy, I contacted the Chief Medical Officer of Health for the province of Ontario who issued a memo to all medical officers of health, warning about the need to encrypt personal health information on portable devices such as USB memory sticks. A more detailed strategy for promoting awareness and compliance among all health information custodians is currently under development and will be finalized early in 2010.

However, enhanced awareness is only part of the solution. As storage capacity increases while costs decrease dramatically, portable storage devices are proliferating in information intensive sectors, such as the health sector. In this environment, it will be a challenge for health information custodians to establish effective management and control over all of their data resources, as well as maintaining effective accountability for the standards required under the Act, and widely expected by the public.

As I have stated over the years, in light of the proliferation of new information and communication technologies, the future of privacy requires a comprehensive and proactive approach, which I have called *Privacy by Design*, whereby both privacy and security are effectively baked into the information eco-system, end-to-end, and throughout the entire

data life-cycle, from initial collection through to final disposal.

While encryption is a key component of any security solution for protecting health information on portable devices, it must be deployed in a holistic and proportional manner in order to be truly effective. Depending on the operating context, some encryption solutions are better than others. Those that are added on, after the fact, requiring users to actively encrypt files by creating passwords or launching a software program every time that health information is stored on a portable device, may be less effective than other encryption solutions. Weak or stolen passwords effectively negate the potential security benefits of encryption. Confusing or complex software interfaces and protocols will also result in users abandoning secure systems and resorting to insecure "workarounds." Users also may be unaware that when encrypted information is transferred from one storage device (e.g., laptop computer) to another (e.g., a USB key), the encryption does not necessarily accompany the data. Once the data is intentionally or unintentionally decrypted back to plaintext, it is out there in plain view, becoming vulnerable to a wide range of unintended uses.

Doing away with mobile devices entirely by locking down all USB ports, in favour of the exclusive use of secure channels and "thin clients," is another approach that may be feasible in some instances but not others. Thin clients, sometimes described as "dumb terminals," are display and input devices which do not process data and input locally, but rather transmit input to a computer to which they are connected and display the resulting output. They often have limited local data storage and output capacities. Since the vast majority of the processing of information is done centrally in such systems, the security risks are generally confined to the central server. However, while it may be easier to manage the security risks, establishing and maintaining secure channels and thin clients tends to be operationally complex and costly to the enterprise, requiring employees to manage identification and authentication credentials in a consistently secure way. Additionally, locking down USB ports across an enterprise may rob an organization of the benefits of connecting other useful, risk-free devices to those ports, such as a mouse or keyboard.

Ideally, organizations should implement enterprise-wide encryption solutions that would only permit the use of authorized portable storage devices to connect to specifically-authorized USB ports, where the encryption is both automatic and seamless. Only devices with authorized USB ports would be able to view, access and decrypt the data stored on an authorized portable storage device. Thus, in the event that an authorized portable storage device was lost or stolen, any personal health information stored on the device would be inaccessible to anyone who found it. Further, it would simply not be possible to use an unauthorized mobile device with such a protected system. The management of this type of arrangement would have to be centralized, easy to set up and administer, and, ideally, low in cost. In addition, all transactions would also need to be logged.

A local Ontario company, CryptoMill, has developed such an enterprise-class security solution that offers this degree of functionality. Their solution called *SEAhawk*, allows organizations to effectively lock down information assets to registered devices only, such as USB memory sticks.

Had such a solution been implemented in Durham Region, the personal health information contained on the USB memory stick that was lost would have been encrypted in a manner that would have locked out all unauthorized parties, only allowing an authorized computer to

decrypt it. Further, any files stored on the USB memory stick would essentially be invisible to anyone who found it or stole it. Anyone, including staff, plugging the USB memory stick into their own computer would either find an encrypted vault – an invisible directory, or else be prompted to format an unrecognized drive, effectively erasing its contents.

If an encrypted USB memory stick was lost, there would be no cause for alarm on the part of the organization, which would have a high degree of confidence that the stored data would not be compromised. There would be no need to invoke the time-consuming and expensive breach management process involving notification, investigation, and remediation.

To their credit, both CryptoMill and Durham Region have been working together non-stop to apply the SEAhawk encryption solution throughout the Durham Region. With the release of this Order, its adoption will be well underway.

Privacy by Design is systemic, embedded, and proactive in nature, thereby serving to prevent privacy mishaps before they occur. It comes *before* the fact of a data breach, not after. While it is true that we cannot eliminate human error, we most certainly *can* eliminate personal information from being revealed, in the process. Human error, in this instance, is not an acceptable excuse. While the loss of a USB memory stick may not have been prevented, the loss of personally identifiable data certainly could have been. Don't blame human error – blame the lack of encryption of easily lost or stolen mobile devices.

CASLPO would like to extend its sincere gratitude to the Information and Privacy Commissioner/Ontario for permission to reprint this information.