Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes

Information & Privacy Commissioner,
Ontario, Canada

Children's Hospital of
Eastern Ontario

September 13, 2011

The Authors of this paper gratefully acknowledge the work of Debra Grant, Senior Health Privacy Specialist, Ontario Information and Privacy Commissioner's Office, in preparing this paper.

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

Table of Contents

Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes

Introduction

Recognizing the positive impact that research may have on the health and welfare of the public and on the operation of the health system, privacy legislation throughout Canada includes provisions that enable health research while simultaneously ensuring the protection of privacy of individuals whose personal information is the subject of research. In Ontario, the *Personal Health Information Protection Act, 2004* ("the *Act*") permits health information custodians ("custodians")[1] to collect, use and disclose personal health information for research purposes, either with the consent of the individual or without the consent of the individual, provided that certain requirements are fulfilled. Without appropriate access to personal health information, much of the health-promoting and life-saving research that is conducted today would not be possible. However, to avoid barriers to such access, there must be public trust and confidence in the ability of the research community to protect the personal health information that is collected, used and disclosed for research purposes.

As we move to an era of electronic records of personal health information, rapid growth in the use of mobile computing and storage devices to collect and store personal health information has posed challenges for the protection of personal health information. Health researchers, in particular, have come to rely heavily on laptop computers, memory sticks and other mobile computing and storage devices ("mobile devices") to collect personal health information in health-care settings and to transfer this information to other devices and locations where it can be analyzed. But, since mobile devices are vulnerable to loss and theft, any personal health information stored on such devices may be exposed to unauthorized collection, use and disclosure, unless reasonable safeguards are implemented to minimize this risk.

1 A health information custodian is defined as a person or organization described in subsection 3(1) of the *Act* with custody or control of personal health information as a result of, or in connection with, the performance of its powers, duties or work. Custodians include health care practitioners; hospitals, including psychiatric facilities; long-term care homes; community care access centres; specimen collection centres, laboratories; independent health facilities; pharmacies; ambulance services; Ontario Agency for Health Protection and Promotion; and the Minister, together with the Ministry of Health and Long-Term Care.

While the theft or loss of mobile devices cannot always be prevented, the loss of personally identifiable health information stored on such devices can be avoided through increased awareness and action on the part of the research community. In particular, unauthorized collection, use and disclosure of personal health information stored on mobile devices could be prevented through the widespread adoption of well-established privacy and security measures, including data minimization and encryption technology.

The primary purpose of this paper is to assist custodians, researchers and research ethics boards in understanding and fulfilling their obligations with respect to safeguarding personal health information that is collected, used and disclosed for research purposes. While the paper highlights the obligations that arise out of the *Act*, it is recognized that there are other legal and professional requirements and guidelines, including the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* and the *ICH Guideline for Good Clinical Practice* that may also apply to the research community. However, while the research community must be aware of other legal and professional requirements and guidelines, they are outside the scope of this paper.

Build in *Privacy by Design*

The paper will highlight two important points. First, custodians, researchers and research ethics boards all have obligations under the *Act* to ensure that appropriate safeguards are in place to protect personal health information that is collected, used or disclosed for research purposes. Second, custodians, researchers and research ethics boards all have opportunities to ensure that appropriate safeguards are in place through the preparation of research plans, the execution of agreements between custodians and researchers, the research ethics board approval process, and the education and training of agents of custodians, including any researchers who may be acting as agents. If all parties involved in the research process were to comply with the requirements of the *Act*, the risks associated with the storage of unencrypted personal health information on mobile devices would be minimized and privacy breaches due to the loss or theft of such devices would be avoided.

To foster public trust and confidence, it is crucial for the research community to take a comprehensive and proactive approach to preventing unauthorized access to unencrypted personal health information on mobile devices. *Privacy by Design* involves embedding privacy directly into the design and operation of information technologies, business practices and related infrastructures, thereby ensuring the highest level of protection. In the context of research, this means that privacy should not only be built into the design and operation of any information technologies that are used, including mobile devices, but also into the design and operation of all research-related practices, including the preparation of research plans, the execution of agreements between custodians and researchers, the research ethics board approval process, and the education and training

of agents of custodians, including any researchers who may be acting as agents. Building privacy into the design of such practices will enable a shift from the traditional zero-sum paradigm (e.g., privacy vs. research) to a positive-sum paradigm, whereby the goal of protecting privacy and the goals of health research can be attained simultaneously. Applying *Privacy by Design* principles creates a win-win scenario so that privacy is protected without compromising health research.

Privacy by Design is proactive in nature. It encompasses a comprehensive approach to information management that ensures that privacy safeguards are already in place when personal health information is first collected, and throughout the entire life cycle. *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal health information is automatically protected – privacy protection is built into the research process *by default*. *Visibility, transparency and respect for privacy are paramount*. *Privacy by Design* seeks to prevent privacy breaches before they occur, rather than prescribing remedial actions. The research community should strive to ensure the principles of *Privacy by Design* are incorporated into the design and implementation of all research-related practices.

Health Research

Health research can provide direct benefits to individuals as well as to society as a whole. Individuals benefit from new treatments and improvements in the quality of care. Society as a whole benefits from improvements in health policy decision-making. An article published in the Bulletin of the World Health Organization[2] concluded that health and biomedical research is an investment that can produce tangible benefits. Through an extensive review of relevant literature, the article explored the relationship between research inputs and health and other outcomes and the value of those outcomes. The article concluded that health and biomedical research has led to:

- Direct cost savings to the health-care system by means of new therapies that reduce either the number of individuals requiring treatment or the cost of treatment;
- Benefits to the economy related to a healthy workforce; and
- Benefits to the economy though commercial development.

High quality research depends on the availability of high quality information. While in some cases de-identified information is sufficient for research purposes, in other cases research questions can only be answered through access to accurate and comprehensive

2 Marin Buxton, Steven Hanney and Teri Jones, *Estimating the Economic Value to Societies of the Impact of Health Research: A Critical Review*, Bulletin of the World Health Organization, 2004, 82:733-739.

personal health information acquired from a number of sources, over an extended period of time. In such cases, personal identifiers are necessary to reliably link information pertaining to a particular individual across sources and time in order to get a complete picture of the health history and the provision of health care to the individual.

While some of the personal health information that is used for research purposes is collected directly from individuals, a substantial portion of the information is acquired indirectly from custodians. Individuals and custodians make personal health information available for research purposes based on the assumption that the research community has the capacity to maintain the confidentiality of the information and to protect the privacy of the individuals to whom the information relates. To avoid privacy and security breaches and thereby maintain public trust, the research community must ensure that strong privacy and security measures are in place and are continuously reassessed in order to mitigate any risks posed by existing and emerging information technologies, including mobile devices.

Privacy in the Context of Personal Health Information

Personal health information is highly personal and sensitive in nature. The unauthorized collection, use or disclosure of personal health information can have serious repercussions for individuals, for custodians and for the health system as a whole.

From the perspective of the individual, a privacy breach may result in stigmatization, discrimination, emotional and psychological harm, loss of trust in the health-care provider and ineligibility or loss of health insurance coverage, employment and housing opportunities or other benefits.

Research has shown that individuals concerned about the inappropriate use and disclosure of their personal health information may engage in privacy-protective behaviours. For example, an individual may withhold or provide incorrect information to his or her health-care provider; avoid seeking treatment or diagnostic testing for certain conditions; or elect to pay for certain drugs and services out-of-pocket rather than submitting a claim through an insurer.[3] To the extent that individuals lack trust in the ability of their health-care provider to protect their personal health information and engage in privacy-protective behaviours, the personal health information that is collected during the course of providing health-care may not be accurate or complete.

3 California HealthCare Foundation, National Consumer Health Privacy Survey 2005, Forrester Research, Inc. available at http://www.chcf.org/

Health care is an information-intensive industry. The delivery of high-quality health care depends on the availability of accurate and complete health information. Accurate and complete information is also essential for conducting high-quality health research and for planning and managing our publicly-funded health system. In other words, the efficient and effective operation of the entire health system rests on the accuracy and quality of the health information collected which, in turn, depends on the confidence that individuals have with respect to the protection of their most sensitive information.

In addition to the potential impact on individuals and the health system, the unauthorized collection, use and disclosure of personal health information may have serious consequences for the responsible custodian. The consequences of privacy breaches may include:

- Fines and lawsuits;
- Damage to the reputation, image and business relationships of the custodian;
- Investigations and proceedings by the Information and Privacy Commissioner of Ontario and/or the regulatory college of the health professional involved in the breach;
- Loss of patient trust and confidence; and
- Costs associated with containing, investigating, remediating and preventing similar breaches; patient notification; and responding to inquiries and complaints.

In short, there is a compelling rationale for investing in proactive measures to prevent privacy breaches, particularly in the context of mobile devices where the high risk of loss or theft is known but relatively easy to mitigate through data minimization and encryption.

Privacy Breaches in the Context of Mobile Devices

The loss or theft of mobile devices containing personal health information is a worldwide problem. In the United States, as required by the *Health Information Technology for Economic and Clinical Health* (HITECH) *Act*, the Secretary of Health and Human Services ("the Secretary") must post a list of breaches of "unsecured protected health information" affecting 500 or more individuals on the website of the Department of Health and Human Services. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary. In the one-year period from September 2009 to September 2010, 164 breaches of unsecured protected health information affecting millions of Americans were posted on the website. As of June 2011, the number of breaches climbed to 288. About

one third of these breaches involved mobile devices, with the vast majority resulting from the loss, theft and/or unauthorized access to personal health information stored on laptop computers.

The theft and loss of mobile devices containing unencrypted personal health information is also a pervasive problem in Ontario. In 2007, the Information and Privacy Commissioner of Ontario ("the Commissioner") issued Order HO-004 after a laptop computer, belonging to a hospital and containing the unencrypted personal health information of 2,900 individuals, was stolen from a vehicle. The personal health information included the individuals' names and hospital numbers, along with information relating to medical conditions. The personal health information had been stored on the laptop computer and transported out of the hospital to be used for research purposes. During the investigation, the hospital acknowledged that identifying personal health information did not need to be removed from the hospital since de-identified information would have been sufficient for the purpose of the research. Also, although the use of identifiable health information for research purposes was a breach of the hospital's policy, the hospital had no mechanism in place to ensure that researchers complied with this policy. Further, the hospital acknowledged that if personal health information had been required for the research project, the researcher could have accessed this information remotely rather than removing it from the hospital on a mobile device.

In 2010, the Commissioner issued Order HO-007 after a USB memory stick containing the unencrypted personal health information of 83,524 individuals who attended H1N1 immunization clinics was lost. The personal health information included the individuals' names, addresses, telephone numbers, dates of birth and health numbers, along with information regarding the individuals' health histories. The investigation revealed that memory sticks were used as a means of transferring personal health information between eight community clinics and the regional headquarters due to problems that were encountered in establishing a Virtual Private Network. A $40 million class action lawsuit has been filed in response to this breach.

Also, in 2010, the Commissioner issued Order HO-008 following the theft of a laptop computer containing the unencrypted personal health information of approximately 20,000 individuals. The information contained on the missing laptop included the individuals' names, medical record numbers and types and dates of surgery and the names of the individuals' health-care providers. The hospital initially believed that the personal health information stored on the laptop was encrypted. However, after the theft occurred, it was determined that despite a hospital policy requiring encryption, the personal health information had not been encrypted due to an error in loading the encryption software onto the laptop computer. In addition, the hospital acknowledged that it was not even necessary to have the records of personal health information stored on the laptop computer.

In short, although there have been a number of orders emphasizing the importance of implementing appropriate safeguards to protect personal health information stored on mobile devices, the theft and loss of mobile devices containing unencrypted personal health information continues to be an ongoing problem throughout the health sector. Unfortunately, the research community has not been immune to such breaches. Action must be taken to avoid further breaches and to help foster public confidence in the ability of the research community to safeguard the personal health information with which they are entrusted.

Complying with the Requirements of the *Act*

There are a number of ways in which custodians may become involved in research. First, custodians may conduct research directly or custodians may authorize one or more of their agents to conduct research on their behalf. An "agent" is defined in section 2 of the *Act* as follows:

> "agent", in relation to a custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated.

A researcher who collects, uses or discloses personal health information with the authorization of the custodian and acts for or on behalf of the custodian in respect of research, and not for the researcher's own purposes, falls within the definition of an "agent" under the *Act*, regardless of whether the researcher has the authority to bind the custodian, is employed by the custodian or is being remunerated.

When research is conducted by the custodian or one or more agents of the custodian using personal health information obtained directly from research subjects or indirectly from another source, this is considered to be a "collection" of personal health information by the custodian. When research is conducted by the custodian or by one or more agents of the custodian, using personal health information previously collected by the custodian, this is considered to be a "use" of personal health information by the custodian.

The second way in which custodians may become involved in research is by making personal health information available to researchers who are conducting research for their own purposes. When a custodian makes personal health information available to a researcher who is not acting on behalf of the custodian, this is considered to be a "disclosure" of personal health information by the custodian.

Regardless of whether the custodian is collecting, using or disclosing personal health information for research purposes, the custodian must comply with the requirements of the *Act* described below.

Duty to Establish Information Practices

Section 10 of the *Act* requires custodians to have in place information practices that comply with the *Act*. They are also required under subsection 16(1) of the *Act* to make available to the public a written statement that provides a general description of the custodian's information practices. Information practices are defined in section 2 of the *Act* as the policy of the custodian for actions in relation to personal health information, including:

(a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and

(b) the administrative, technical and physical safeguards and practices the custodian maintains with respect to the information.

Custodians should develop and implement comprehensive policies and accompanying procedures that set out the expectations and requirements for all agents, including researchers, in respect of the storage and transporting of personal health information on mobile devices. For example, the policy should specify whether agents are permitted to retain or transport personal health information on a mobile device. If permitted to do so, at a minimum, the policy should require that only the minimum amount of personal health information be stored for the minimum amount of time necessary and that the personal health information be strongly encrypted. In addition, the policy should set out the circumstances in which personal health information is permitted to be retained or transported on a mobile device, the procedure to be followed in storing or transporting personal health information on a mobile device, and the conditions or restrictions that will be imposed on the retention or transporting of personal health information on a mobile device. The policy should also specify the disciplinary action that will be taken if the policy is breached.

Written policies and procedures are critical as they formalize and clarify the required practices in relation to the use of mobile devices. Further, in the event that there is a privacy breach involving a mobile device, to determine whether the custodian has complied with the *Act*, the Information and Privacy Commissioner of Ontario may review the custodian's written information practices, including policies and procedures with respect to mobile devices, along with any agreements that are in place.

Researchers who are acting as agents of a custodian should be bound by the policies and procedures of the custodian through confidentiality agreements or other contractual arrangements. Such agreements should be robust, comprehensive and updated on a regular basis to reflect any changes to the health information custodian's written policies and procedures and to address any emerging threats to privacy and security. For more guidance related to confidentiality agreements, please refer to the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* on the website of the Office of the Information and Privacy Commissioner of Ontario.

Data Minimization

As a general rule, custodians are required to minimize the amount of personal health information that they collect, use and disclose. Specifically, section 30 of the *Act* requires custodians not to collect, use or disclose personal health information if other information would serve the purpose and not to collect, use or disclose more personal health information than is reasonably necessary to meet the purpose. For example, if de-identified or aggregate information is sufficient for the purpose, custodians must not collect, use or disclose personal health information. With limited exceptions, these data minimization requirements apply at all times, including in the context of the collection, use and disclosure of personal health information for research purposes. Compliance by custodians with the data minimization requirements of the *Act*, which reflect internationally accepted fair information practices,[4] will help to minimize the likelihood of personal health information being stored on mobile devices. Data minimization is particularly relevant in the context of mobile devices where "endpoint security"[5] presents an ongoing challenge in a world of endless connections.

Security

Subsection 12(1) of the *Act* imposes a general obligation on custodians to take steps that are reasonable in the circumstances to ensure that personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal. Subsection 13(1) further requires custodians to ensure that records of personal health information in their custody or under their control are retained, transferred and disposed of in a secure manner. In general, these security requirements, which reflect internationally accepted fair information practices, apply

4 Fair information practices are a set of widely accepted principles governing the collection, use and disclosure of personal information that form the basis of privacy codes and privacy legislation throughout the world.

5 Endpoint security is a strategy in which security software is distributed to end-user devices, such as mobile devices, but managed centrally.

at all times, including when personal health information is collected, used or disclosed for research purposes.

In determining what steps are reasonable in the circumstances to safeguard personal health information, custodians should consider any orders, guidelines, fact sheets and best practices issued by the Office of the Information and Privacy Commissioner of Ontario ("IPC") under the *Act* and Regulation 329/04 to the *Act* ("the Regulation"), as well as evolving industry standards and best practices. In general, given the sensitivity of personal health information and the serious consequences of breaches of such information, the IPC expects custodians to implement strong safeguards to protect personal health information. The guidance that has been provided to date by the IPC with respect to safeguarding personal health information stored or transported using mobile devices is summarized below.

Avoid Storing and Transporting Personal Health Information on Mobile Devices

As a first line of defence against unauthorized access to personal health information, the storage or transporting of personally identifiable health information on such devices should be avoided. In the context of research, this means that, to the greatest extent possible, research plans that require the use of mobile devices to store or transport personal health information should be avoided and alternatives considered.

Alternatives include refraining from storing unencrypted personal health information on mobile devices and using aggregate or de-identified information so that the identities of the individuals whose information is stored or transported on the mobile device could not be readily ascertained if the information were accessed by unauthorized persons. Other alternatives include accessing the personal health information remotely and securely through a Virtual Private Network and dedicated "thin client" (i.e., a computer that has limited functionality but rather depends heavily on its central server for information processing functions).

Use Strong Passwords

If it is necessary to store or transport personal health information on a mobile device, the device must be protected through the use of a strong password that is kept secret. Strong login passwords are usually characterized by no dictionary words; a combination of letters, numbers and symbols; and eight or more characters, with 14 or more being ideal.

But, while passwords are an important line of defence against unauthorized access, they are not, in and of themselves, sufficient. Passwords may be written down, stolen, shared, hacked or cracked with readily available software.

Since it is not impossible to effectively guard against the infinite number of security vulnerabilities that currently exist and no single solution will protect against all vulnerabilities, resources must be devoted to developing complementary capabilities that will prevent the most likely attacks. This concept is referred to as "defence in depth" security. As an example, Intel has developed a model for a defence in depth strategy that involves prediction, prevention, detection, and response.[6] Prediction requires an organization to understand why the organization would be attacked, who the potential attackers may be, the methods of attack that may be used and the most probable targets. Prevention requires the implementation of a combination of technical and behavioural controls to deter and prevent most attacks. Detection requires that security incidents be identified and contained and that intruders be eliminated as future threats. Response requires swift and effective action to minimize the impact of a security incident and restore the organization to a normal state.

Thus, strong passwords should be complemented by defence in depth security measures such as requiring individuals to change their passwords on a regular basis and automatic device lock-out or even deletion of the contents of a mobile device after a defined number of failed login attempts. Also, it is generally recommended that a single password not be used to access both the mobile device and the personal health information stored on the mobile device.

Use Strong Encryption

Mobile devices should never contain unencrypted personal health information. Encryption is a process by which ordinary text or data, referred to as 'plaintext,' is turned into an unintelligible stream of seemingly random symbols, referred to as 'cyphertext.' This process is controlled by a digital 'key,' which will allow access to the encrypted information.

The key could be something you know, such as a strong password which is separate and distinct from the login password; or something you have, such as a separate hardware or software "token" that you carry; or something about you, such as your fingerprint scan or other measurable biometric or behavioural attribute. Without the key, the information is unreadable. The effectiveness of encryption depends on the encryption standard, as well as the strength and secrecy of the key(s) used.

To be effective, encryption must be deployed in a holistic and proportional manner taking into account all identified risks and the operational environment. For example, it is not sufficient to encrypt the information on one device, if information will be transferred to and from other unencrypted devices. Users may be unaware that when encrypted information is transferred from one storage device (e.g., laptop computer) to another (e.g., a USB memory stick), the encryption does not necessarily accompany the

6 Matthew Rosenquist, *Intel White Paper: Defense in Depth Strategy Optimizes Security*, September 2008.

information. Once the information is intentionally or unintentionally decrypted back to plaintext, it becomes vulnerable to a wide range of risks.

Depending on the specific context, some encryption solutions are better than others. Encryption solutions that are added on, after the fact, and which require users to actively encrypt files by creating passwords or require users to launch a software program every time personal health information is stored on a mobile device, may be less effective. As noted above in the context of login passwords, weak, stolen or shared passwords that are used as keys to access encrypted data effectively negate the potential security benefits of encryption. Confusing or complex software interfaces and protocols may also result in users abandoning secure systems and resorting to insecure workarounds.

Strong encryption requires minimum technical and functional requirements. Encryption algorithms must be designed to meet a recognized standard, and encryption products should be independently validated to ensure that they are designed and implemented properly. Authorized users should be properly registered, trained and equipped. Users who are authorized to decrypt the information must be securely authenticated by means of passwords, biometrics, or security tokens. Once the encryption system is deployed, the encryption keys must be protected and managed effectively. This will help to ensure that personal health information remains available throughout its life cycle, regardless of forgotten passwords or misplaced security tokens. The encryption system's protections should be operational by default, without users being required to take special steps to ensure that the information remains encrypted. Information technology infrastructures that use security technologies such as encryption should be subject to a Threat and Risk Assessment prior to live operations (and preferably prior to implementation) to ensure that they function as expected. Further details on technical and functional requirements for strong encryption can be found in *Fact Sheet #16 - Health-Care Requirement for Strong Encryption* available on the website of the Office of the Information and Privacy Commissioner of Ontario.

Duty to Inform Agents

Subsection 17(1) of the *Act* allows a custodian to permit its agents to collect, use, disclose, retain or dispose of personal health information on behalf of the custodian only if the custodian is permitted or required to collect, use, disclose, retain or dispose of the information and the collection, use, disclosure, retention or disposition of the information is in the course of the agent's duties and not contrary to the limits imposed by the custodian, the *Act* or another law.

Since a custodian is ultimately accountable for the collection, use, disclosure, retention and disposal of personal health information by its agent, the custodian or a designated contact person must ensure that all agents of the custodian are appropriately informed of

their duties under the *Act*. These duties include compliance with the data minimization and security requirements described above and, in the case of researchers, compliance with the requirements of the *Act* that apply specifically to research as described below.

In informing agents of their duties under the *Act*, the custodian or a designated contact person should ensure that agents, including any researchers who are acting as agents, are aware of the risks associated with the use of mobile devices and the policies, procedures and practices of the custodian that are in place to minimize these risks. This information should be actively and effectively communicated to researchers. Researchers should also be repeatedly reminded of their responsibilities when dealing with mobile devices and the need for proper safeguards to protect personal health information on such devices.

Comprehensive, ongoing, role-based privacy and security training pertaining to the risks posed by the deployment and use of mobile devices must be developed and implemented. Training should be tailored to meet the needs of researchers. Since agents of the custodian will change over time, privacy and security training must be provided on an ongoing basis. Also, since technology is constantly evolving, privacy and security education and training must be updated on a regular basis to address any new threats to privacy and security.

Custodians should ensure that their agents not only understand how to apply, but also have the capacity to apply the policies, procedures and practices with respect to mobile devices in their day-to-day work. This can be accomplished by providing appropriate training, tools and resources.

Since the custodian is ultimately accountable for the collection, use and disclosure of personal health information by its agents, the custodian should be able to demonstrate that its agents are complying with the policies, procedures and practices of the custodian with respect to mobile devices. This may be accomplished through a robust audit program to monitor compliance. Remedial action, including any necessary and appropriate disciplinary action, should be taken in the event of a breach.

In order to inform agents of their duties under the *Act*, the custodian must first identify its agents. Where personal health information is made available for research purposes, the custodian must determine whether the researcher is acting as an agent of the custodian in conducting the research, or if the research is being conducted for the researcher's own purposes. This is important since the obligations of the custodian vary depending on whether personal health information is being "used" by an agent of the custodian or "disclosed" to a researcher who is conducting the research for the researcher's own purposes.

In some cases, it may not be clear if a researcher, who is affiliated with a custodian, is acting for or on behalf of the custodian in conducting research. This is because the researcher may have traditionally conducted research independently of the custodian; the researcher may be affiliated with another organization, such as an academic institution; and/or the researcher may obtain funding and equipment, such as mobile devices, through sources other than the custodian. Thus, there could be challenges in imposing requirements on such researchers, even in cases where the custodian determines that the researcher is acting as an agent of the custodian in conducting the research.

Nonetheless, since custodians are ultimately accountable for the collection, use, disclosure, retention and disposal of personal health information by their agents, they will be accountable for any privacy breaches caused by researchers who are acting as agents. Therefore, custodians must identify which researchers are acting as their agents and take reasonable steps to ensure that such researchers are informed about their duties under the *Act*.

Also, to avoid any misunderstandings about the chain of accountability, once the relationship between the researcher and the custodian has been determined, it should be formally documented through a confidentiality agreement or other contractual agreement.

Research Requirements

Section 29 of the *Act* permits custodians to collect, use and disclose personal health information if the individual consents or if the *Act* permits or requires the collection, use or disclosure to be made without the consent of the individual. In the context of research, custodians may collect, use and disclose personal health information for research purposes either with the consent of the individual or without the consent of the individual provided that all of the requirements of the *Act* are satisfied. These requirements include the general requirements described above, as well as the requirements that apply specifically in the context of research described below.

Research with Consent

When collecting, using or disclosing personal health information for research purposes with the consent of the individual, a custodian must ensure that all the required elements of consent, set out in section 18 of the *Act*, have been fulfilled. Specifically, the consent:

- must be a consent of the individual;
- must be knowledgeable;
- must relate to the information; and
- must not be obtained through deception or coercion.

Consent to the collection, use or disclosure of personal health information is knowledgeable if it is reasonable in the circumstances to believe that the individual knows the purposes of the collection, use or disclosure, as the case may be, and that the individual may give or withhold consent.

Research without Consent

When collecting, using or disclosing personal health information for research purposes without the consent of the individual, a custodian must satisfy other requirements of the *Act*. These requirements vary depending on whether the research is being conducted by or on behalf of the custodian, in which case the personal health information is being *collected* and/or *used* by the custodian for research purposes, or whether the personal health information is being provided to a researcher who is conducting the research for his or her own purposes, in which case the personal health information is being *disclosed* to the researcher by the custodian.

Where the research is being conducted by or on behalf of the custodian, the custodian is responsible for ensuring that all the requirements relating to collection and use of personal health information for research purposes are satisfied. Where the research is being conducted for the researcher's own purposes, the custodian must ensure that all the requirements relating to the disclosure of personal health information for research purposes are satisfied.

Collection

Subsection 36(1)(d) of the *Act* permits a custodian or an agent of a custodian to collect personal health information, without consent, from someone who is not a custodian for the purposes of research provided that the requirements for the use or disclosure of personal health information for research purposes without consent, as may be applicable, are satisfied. These requirements include the preparation of a written research plan and approval of the research plan by a research ethics board.

Further, subsection 36(1)(g) of the *Act* permits a custodian or an agent of a custodian to collect personal health information from a person who is permitted or required by law to disclose the information to the custodian. Since custodians are permitted to disclose personal health information for research purposes in accordance with section 44 of the *Act*, this means that a custodian may also collect personal health information from another custodian without consent for research purposes provided that the custodian that discloses the personal health information satisfies all the requirements of section 44 of the *Act*, as described below.

Use

Subsections 37(1)(j) and 37(3) of the *Act* permit a custodian or an agent of a custodian to use personal health information, without consent, for research purposes, provided that certain requirements are satisfied. The requirements that must be satisfied are set out in subsections 44(2) to 44(4) and subsection 44(6)(a) to (f) of the *Act* and include the preparation of a written research plan and approval of the research plan by a research ethics board, as described below.

Disclosure

Section 44 of the *Act* permits a custodian to disclose personal health information, without consent, for research purposes provided that the requirements of section 44 of the *Act* have been satisfied. Section 44 of *Act* requires researchers who wish to receive personal health information from a custodian to submit to the custodian a written application, a research plan that meets the requirements of the *Act* and the Regulation and a copy of the decision of the research ethics board approving the research plan. They must also comply with the requirements in subsection 44(6) of the *Act* and enter into an agreement with the custodian in which the researcher agrees to comply with the conditions and restrictions, if any, that the custodian imposes relating to the use, security, disclosure, return or disposal of the personal health information.

Research Plans

Before a custodian may collect, use or disclose personal health information for research purposes, without consent, the person conducting the research is required to prepare a research plan that meets the requirements of the *Act* and the Regulation.

Subsection 44(2) of the *Act* requires the research plan to be in writing and to set out the affiliation of each person involved in the research, the nature and objectives of the research and the public or scientific benefit of the research that the researcher anticipates.

Section 16 of the Regulation outlines additional requirements that must be addressed in a research plan. One of the requirements is that the researcher must explain why the research cannot reasonably be accomplished without the personal health information and, if personal health information is required, the safeguards that the researcher will impose to protect the confidentiality and security of the personal health information, including an estimate of how long the personal health information will be retained in an identifiable form, and why.

In order to satisfy these requirements, researchers must justify each element of personal health information that they are proposing to collect, use or disclose and provide an estimate of how long the personal health information will be retained in identifiable form and why. To the extent that researchers only collect, use and disclose personal health information when it is necessary to do so and de-identify the personal health information at the first reasonable opportunity, the likelihood of personal health information being stored or transported on mobile devices would be minimized.

Researchers must also describe the safeguards that will be put in place to protect personal health information. This should include the safeguards that will be put in place to protect personal health information that the researcher intends to store or transport using mobile devices. In determining what safeguards to include in their written research plans, researchers should heed the guidance provided by the Office of the Information and Privacy Commissioner of Ontario under the *Act* and the Regulation, as well as evolving industry standards and best practices. Where the researcher is a custodian or acting as an agent of a custodian, the required safeguards that are incorporated into the research plan should reflect the policies, procedures and practices implemented by the custodian.

It is important to note that the provisions in the *Act* that permit the collection, use and disclosure of personal health information for research purposes are permissive rather than mandatory, meaning that custodians must exercise discretion in deciding whether to collect, use or disclose personal health information for such purposes. In exercising this discretion, custodians should take into consideration the safeguards that will be implemented to protect personal health information. Custodians should only permit personal health information to be made available for research purposes in cases where strong privacy and security measures have been incorporated into the research plan to protect the confidentiality of the information and the privacy of individuals with respect to their personal health information, including personal health information stored or transported using mobile devices.

Research Ethics Board Approval

Before a custodian may collect, use or disclose personal health information for research purposes, without consent, the written research plan must be approved by a research ethics board. A "research ethics board" is defined in section 2 of the *Act* as a board of persons that is established for the purposes of approving research plans under section 44 of the *Act* and that meets the prescribed requirements.[7]

7 The prescribed requirements are set out in section 15 of the Regulation, which states that the research ethics board must have at least five members, each with specific characteristics and/or areas of expertise, and that the research ethics board must only act where there is no conflict of interest between its duty under the *Act* and any participating board member's personal interest in the disclosure of the personal health information or in the performance of the research.

In deciding whether to approve a research plan, the research ethics board is required to consider the factors set out in subsection 44(2) of the *Act*, including whether the objectives of the research could reasonably be accomplished without using the personal health information that is to be disclosed and whether, at the time the research is conducted, adequate safeguards will be in place to protect privacy and preserve confidentiality. This means that research ethics boards must first consider whether the research can be carried out using aggregate or de-identified information rather than personal health information. To the extent that research ethics boards only approve research plans that limit the collection, use and disclosure of personal health information to that which is necessary to accomplish the research purpose, the likelihood of personal health information being stored or transported on mobile devices would be minimized.

In cases where a research ethics board has determined that the objectives of the research could not reasonably be accomplished without using personal health information, it must then determine whether adequate safeguards will be in place to preserve the confidentiality of the information and to protect the privacy of individuals with respect to this information. In determining whether adequate safeguards will be in place, a research ethics board should consider guidance that has been provided by the Office of the Information and Privacy Commissioner of Ontario under the *Act* and the Regulation, as well as evolving industry standards and best practices. To the extent that research ethics boards only approve research plans that incorporate adequate safeguards to protect personal health information, the likelihood of unauthorized access to any personal health information stored on a mobile device, that happens to be lost or stolen, would be reduced.

Although there is no requirement in the *Act* to have a research ethics board approve a research plan when a custodian collects, uses or discloses personal health information for research purposes with the consent of the individual, research plans often must be approved by a research ethics board in order to satisfy the requirements of sponsors, funders, publishers, and data providers. Further, individuals may not wish to participate in research that has not been reviewed by a research ethics board. Thus, regardless of whether the research is conducted with or without consent and regardless of whether the *Act* requires a research ethics board to approve the research plan, research ethics boards will in most cases have an opportunity to review research plans. Research ethics boards will be in a position to ensure that the collection, use and disclosure of personal health information is limited to that which is necessary and that appropriate safeguards are in place to protect personal health information at all times, including when personal health information is stored on mobile devices. This will minimize the likelihood of personal health information being stored or transported on mobile devices and, in those cases where it is necessary to store or transport personal health information on such devices, it will minimize the risk of unauthorized access to personal health information if the mobile device is lost or stolen.

Agreements

Before making personal health information available to a researcher who is not acting as an agent, the custodian must enter into an agreement with the researcher in which the researcher agrees to comply with the conditions and restrictions, if any, that the custodian imposes relating to the use, security, disclosure, return or disposal of the personal health information. Custodians should ensure that appropriate conditions and restrictions relating to the security of personal health information, including safeguards for any personal health information that may be stored or transported on mobile devices, are incorporated into their agreements with researchers. These conditions and restrictions should reflect the guidance that has been provided by the Office of the Information and Privacy Commissioner of Ontario in the context of mobile devices.

Research agreements that are used to bind researchers to the requirement to implement adequate safeguards should be robust, comprehensive and updated on a regular basis to reflect any changes to the health information custodian's written policies and procedures and to address any emerging threats to privacy and security. For a research agreement template, please refer to the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*.

Compliance by Researchers

A researcher who obtains personal health information from a custodian for the purpose of conducting research on behalf of the custodian or for the researcher's own purposes must:

- comply with any conditions specified by the research ethics board;
- use the information only for the purposes set out in the research plan approved by the research ethics board;
- not publish the information in a form that could reasonably enable a person to ascertain the identity of the individual;
- not disclose the information except as required by law or as permitted by the Regulation;
- not make contact or attempt to make contact with the individual, directly or indirectly, unless the custodian first obtains consent;
- notify the custodian immediately in writing if the researcher becomes aware of any breach of these requirements; and
- comply with the agreement, in cases where an agreement with the custodian is required.

Recipient Rule

Researchers who are not custodians or agents of a custodian but who receive personal health information from a custodian, with or without the consent of the individual, are bound by the data minimization rule that applies to all recipients of personal health information. Specifically, subsection 49(2) of the *Act* prohibits a recipient from using or disclosing more personal health information than is reasonably necessary to meet the purpose, unless the use or disclosure is required by law. This means that if de-identified or aggregate information is sufficient for the purpose, then the researcher is obliged not to use or disclose personal health information. Compliance with subsection 49(2) of the *Act* by researchers who are recipients of personal health information will help to minimize the likelihood of personal health information being stored or transported on mobile devices.

Conclusion

The loss or theft of mobile devices containing personal health information continues to be an ongoing problem in the health sector. Breaches of personal health information stored on mobile devices can have serious repercussions for individuals, for the researchers and custodians who are responsible for such breaches and for the health system, as a whole, which relies on the availability of accurate and complete personal health information. While the theft or loss of mobile devices cannot always be prevented, unauthorized collection, use and disclosure of personal health information stored on mobile devices could be avoided through the widespread adoption of well-established privacy and security measures, including data minimization and encryption technology.

Custodians, researchers and research ethics boards all have obligations under the *Act* to ensure that appropriate safeguards are in place to protect personal health information that is collected, used or disclosed for research purposes. Further, custodians, researchers and research ethics boards all have opportunities to ensure that appropriate safeguards are in place through the preparation of research plans, the execution of agreements between custodians and researchers, the research ethics board approval process, and the education and training of agents of custodians, including any researchers who may be acting as agents. Using the principles of *Privacy by Design*, the safeguards that have been articulated by the Office of the Information and Privacy Commissioner of Ontario in the context of mobile devices should be incorporated into the standard practices of the research community.

Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
CANADA

Telephone: (416) 326-3333
Toll-free: 1-800-387-0073
Fax: (416) 325-9195
TTY (Teletypewriter): (416) 325-7539
Website: www.ipc.on.ca
E-mail: info@ipc.on.ca