What to do When Faced With a Privacy Breach:

Guidelines for the Health Sector

ANN CAVOUKIAN, PH.D.
COMMISSIONER

INFORMATION AND PRIVACY
COMMISSIONER/ONTARIO

Table of Contents

What is a privacy breach? 1

What are the benefits of having a "privacy breach protocol?" 2

Guidelines on what health information custodians should do 2

- Step 1: Respond immediately by implementing the privacy breach protocol 2
- Step 2: Containment - Identify the scope of the potential breach and take steps to contain it 2
- Step 3: Notification - Identify those individuals whose privacy was breached and notify them of the breach 2
- Step 4: Investigation and Remediation 3

What happens when the IPC investigates a privacy breach? 3

What steps can you take to avoid a privacy breach? 4

IPC website 4

What to do When Faced With a Privacy Breach: Guidelines for the Health Sector

The *Personal Health Information Protection Act, 2004* (the *Act*) sets out the rules that persons or organizations defined as "health information custodians" must follow when collecting, using, disclosing, retaining and disposing of personal health information.

The rules recognize the unique character of personal health information as one of the most sensitive types of personal information that is frequently shared for a variety of purposes, including care and treatment, health research, and managing our publicly funded health care system.

The *Act* balances individuals' right to privacy with respect to their own personal health information with the legitimate needs of health information custodians to collect, use and share this information. With limited exceptions, the *Act* requires health information custodians to obtain consent before they collect, use or disclose personal health information. The *Act* also makes health information custodians responsible for the secure storage and destruction of personal health information. In addition, individuals have the right to access and request correction of their own personal health information.

The purpose of this paper is to provide guidance to health information custodians when they are faced with a "privacy breach."

WHAT IS A PRIVACY BREACH?

A privacy breach occurs whenever a person has contravened or is about to contravene a provision of the *Act* or its regulations, including section 12(1) of the *Act*.

Section 12(1) of the *Act* requires health information custodians to take steps that are reasonable in the circumstances to ensure personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

A health information custodian may become aware of a privacy breach in a number of ways. The custodian may be contacted by the Office of the Information and Privacy Commissioner (IPC) when a formal complaint has been filed by a member of the public, or where the Information and Privacy Commissioner initiates her own investigation. The health information custodian may also become aware of a breach during the normal course of business (self-identification).

This paper will concentrate on situations where the health information custodian has self-identified the privacy breach or the health information custodian has been contacted by the IPC regarding a potential breach. This will generally be a situation where personal health information is stolen, lost or accessed by unauthorized persons. Many of these situations will involve unintentional breaches of the *Act*. For example, personal health information may be lost (a file is misplaced), stolen (laptop computers are a prime example) or inadvertently disclosed to an unauthorized person in error (a letter addressed to patient A is actually mailed to patient B). On the other hand, the health information custodian may become aware of breaches that may be intentional; for example, the unauthorized access of patient files by staff.

In these cases, the health information custodian is encouraged to report the incidents to the IPC so that assistance can be provided in fulfilling their obligations under the *Act* (e.g. notification) and to take whatever remedial steps are necessary to prevent future similar occurrences. The IPC recommends that a health information custodian develop a "privacy breach protocol" which includes the actions outlined below.

WHAT ARE THE BENEFITS OF HAVING A "PRIVACY BREACH PROTOCOL?"

- Health information custodians can respond quickly and in a coordinated manner;
- Roles and responsibilities of staff will be clarified;
- A process for effective investigations will be documented;
- Effective containment of the breach will be aided;
- Remediation efforts will be easier; and
- Health information custodians will be prepared for the potential involvement by the IPC.

GUIDELINES ON WHAT HEALTH INFORMATION CUSTODIANS SHOULD DO

Upon learning of a privacy breach, immediate action must be taken. Many of the following guidelines need to be carried out simultaneously or in quick succession.

Step 1: Respond immediately by implementing the privacy breach protocol

- Ensure appropriate staff within your organization are immediately notified of the breach, including the Chief Privacy Officer or contact person for the purposes of the *Act*;
- Depending on the nature or seriousness of the privacy breach, there may be a need to contact senior management, patient relations or the information and technology and/or communications department within your organization;
- Inform the IPC Registrar of the privacy breach and work together constructively with IPC staff; and
- Address the priorities of containment and notification as set out in the following steps.

Step 2: Containment – Identify the scope of the potential breach and take steps to contain it

- Retrieve the hard copies of any personal health information that has been disclosed;
- Ensure that no copies of the personal health information have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required; and
- Determine whether the privacy breach would allow unauthorized access to any other personal health information (e.g. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system).

Step 3: Notification – Identify those individuals whose privacy was breached and notify them of the breach

- The *Act* requires health information custodians to notify individuals, at the first reasonable opportunity, but does not specify the manner in which notification must be carried out;

- For example, notification can be by telephone or in writing, or depending on the circumstances, a notation made in the individual's file to be discussed at his/her next appointment;
- There are numerous factors that may need to be taken into consideration when deciding on the best form of notification (e.g. the sensitivity of the personal health information). As a result, the health information custodian may want to contact the IPC to discuss the most appropriate form of notification;
- There may also be exceptional circumstances when the health information custodian may want to discuss notification with the IPC before proceeding (e.g. when notification is not possible or may be detrimental to the individual). If this is the case, the health information custodian is encouraged to contact the IPC to discuss these circumstances;
- When notifying individuals affected by the breach, provide details of the extent of the breach and the specifics of the personal health information at issue;
- Advise affected individuals of the steps that have been or will be taken to address the breach, both immediate and long-term; and
- Advise that the IPC has been contacted to ensure that all obligations under the *Act* are fulfilled (where applicable).

Step 4: Investigation and Remediation

- Conduct an internal investigation into the matter. The objectives of the investigation are to: 1) ensure the immediate requirements of containment and notification have been addressed; 2) review the circumstances surrounding the breach; and 3) review the adequacy of existing policies and procedures in protecting personal health information;
- Address the situation on a systemic basis. In some cases, program-wide procedures may warrant review (e.g. a misdirected fax transmission);
- Advise the IPC of your findings and work together to make any necessary changes;
- Ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of the *Act*; and
- Cooperate in any further investigation into the incident undertaken by the IPC.

WHAT HAPPENS WHEN THE IPC INVESTIGATES A PRIVACY BREACH?

When investigating a privacy breach, the IPC will, depending on the circumstances:

- Ensure any issues surrounding containment and notification have been addressed;
- Interview individuals involved with the privacy breach or individuals who can provide information about a process;
- Obtain and review the health information custodian's position on the privacy breach;
- Ask for a status report of any actions taken by the health information custodian;

- Review and provide input and advice on current policies and procedures and any other relevant documents and recommend changes; and
- If appropriate or necessary, issue a report or order at the conclusion of the review.

WHAT STEPS CAN YOU TAKE TO AVOID A PRIVACY BREACH?

Health information custodians governed by the *Act* would be well served by adopting proactive measures to prevent a privacy breach from occurring. These measures should include:

- Educating staff about the privacy rules governing the collection, retention, use and disclosure of personal health information set out in the *Act*;
- Educating staff about the privacy rules governing safe and secure disposal of personal health information and the security of records;
- Ensuring policies and procedures are in place that comply with the privacy protection provisions of the *Act* and that staff are properly trained in this respect;
- Safeguarding personal health information when it is physically removed from the office or institution; for example, by ensuring that all laptops and PDA's are password protected and data is encrypted;
- Ensuring that a baseline of logging and auditing is in place on all systems, particularly those containing electronic health records and that staff are aware that regular audits will occur;
- Conducting a privacy impact assessment (PIA), where appropriate. The PIA is a process that helps determine whether new technologies, information systems and proposed programs or policies meet basic privacy requirements [For further information, see the IPC publication entitled *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, available on the website];
- When in doubt, obtaining advice from your organization's legal department and Chief Privacy Officer; and
- Consulting with the IPC's Policy and Compliance Department in appropriate situations.

IPC WEBSITE (WWW.IPC.ON.CA)

Resolution Summaries and Reports or Orders that are publicly available with respect to matters that the IPC has investigated are accessible through the IPC's website at www.ipc.on.ca. They may be located via the Orders and Complaint Reports section or by using the search function.

Information about the IPC's privacy complaint process can be found in the "About Us – How Things Work" section of the website.

In addition, the IPC has published a number of documents that can assist health information custodians, which are also available on the website:

Frequently Asked Questions: Personal Health Information Protection Act (PDF format)

The Personal Health Information Protection Act and Your Privacy (PDF format)

A Guide to the Personal Health Information Protection Act (PDF format)

Your Health Information: Your Rights - Your Guide to the Personal Health Information Protection Act, 2004 - A joint publication of the Ministry of Health and the IPC (PDF format)

Your Health Information and Your Privacy in Our Facility

Your Health Information and Your Privacy in Our Office

Your Health Information and Your Privacy in Our Hospital

Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act

Access/Correction Complaint Flow Chart

Collection, Use, Disclosure Complaint Flow Chart

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone : 416-326-3333 or 1-800-387-0073
Fax : 416-325-9195
TTY (Teletypewriter) : 416-325-7539
Website : www.ipc.on.ca
Email : info@ipc.on.ca