ICHA | Inner City Health Associates

Privacy Breach Protocol

ICHA is the owner and administrator of the OSCAR EMR used by ICHA physicians and staff, and by ICHA partner agencies. ICHA is both a Health Information Custodian (HIC) and a Health Information Network Provider (HINP). ICHA works with many partner agencies, and each agency is responsible for its own privacy and security policies and protocols. Each agency's policy should meet the requirements of this protocol in the case of a privacy breach involving an ICHA patient or personal health information included in the ICHA EMR. This protocol will focus on situations where ICHA either receives a self report, or has been contacted by a partner agency, individual or by the Information Privacy Commissioner (IPC) regarding a potential breach.

Understanding a Privacy Breach

A privacy breach occurs when a person contravenes or is about to contravene a rule under the Personal Health Information Protection Act, 2004 (PHIPA) or ICHA's privacy policies. These breaches happen when patient information is lost, stolen or accessed by someone without authorization. These include:

- A fax is misdirected
- An unencrypted laptop or mobile device with health information saved on the hard drive is stolen
- A courier package is not delivered to the correct address
- A USB key is lost
- A patient reads another patient's health record on a computer while waiting in a clinic room
- A test result is filed in the wrong health record
- Someone talks about an ICHA patient with someone who is not a part of the circle of care
- A laptop used for an ICHA clinic is also used for a workshop at the shelter, and a participant opens documents from the desktop which contain personal health information of other clients at the Shelter.
- Health records are disposed of as recycling after being faxed to ICHA and are not cross-cut shredded
- Health information is given to the media without consent

Privacy Breach Protocol[1]

The first agency to discover a breach involving ICHA data will immediately notify the ICHA Privacy Officer in addition to any other notifications required by the agency's own breach protocol. If an ICHA physician or staff member discovers the potential breach, immediate steps to contain the breach will be taken, and the ICHA Privacy Officer notified. Where ICHA confirms a breach it will immediately notify all affected agencies.

Responding to a breach, when detected, requires immediate action. This may require the creation of a breach response team from several agencies with ICHA. The 4 steps identified in this protocol may be carried out simultaneously or sequentially:

<u>Step 1:</u> Respond immediately by implementing the privacy breach protocol

- Ensure the ICHA Privacy Officer is immediately notified. S/He is responsible for ensuring that the appropriate staff within ICHA are notified of the breach, including the Medical Director.
- The Medical Director is responsible for determining if the Board of Directors needs to be informed.
- Determine which agencies are affected and notify them as appropriate,
- Determine if the IPC Registrar should be informed of the privacy breach and if so, work together constructively with IPC staff; and
- Address the priorities of containment and notification as set out in the following steps.

<u>Step 2</u>: 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 this person's contact information in the event that follow-up is required;
- Determine whether the privacy breach would allow unauthorized access to any other personal health information (e.g. electronic medical record) and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system).
- If it appears that the breach was intentional, or the result of negligence, the ICHA Privacy Officer will immediately notify the appropriate management personnel and provide assistance to ascertain whether disciplinary measures are appropriate. If the breach appears to be the result of illegal activity, the police will be notified.

[1] Based on the information and Privacy Commissioner/Ontario "What to Do When Faced with a Privacy Breach? Guidelines for the Health Sector". Available online: http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf

<u>Step 3</u>: Notification

- Where other HICs are involved, consult with and identify the HIC or HICs that will lead in notification.
- The Act requires that individuals affected by the breach are notified at the first reasonable opportunity, but does not specify the manner in which notification must be carried out;
- Notification will first be discussed by the notifying Privacy Officer with the MRP of the individual to ensure that notification will not be harmful to the individual. If this is felt to be the case, the notifying HIC will contact the IPC to discuss these circumstances.
- Determine the best manner in which to do the notification. Where feasible, this will generally mean asking the MRP to inform in person the individual affected, with the presence of the Privacy Officer where needed.
- 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.

<u>Step 4</u>: 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);
- 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.
- The ICHA Privacy Officer is responsible for the completion of a written report of the incident and ensuring that documentation regarding the notification and response to the breach are retained and filed in a secure manner. The report will be shared with affected agencies once complete.

Reference Material

Information and Privacy Commissioner/Ontario

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

(http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=433)

Breach Notification Assessment Tool

(http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=581)

Privacy Commissioner of Canada

Key Steps for Organizations in Responding to Privacy Breaches

(http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp)

Privacy Breach Checklist

(http://www.privcom.gc.ca/information/guide/2007/gl_070801_checklist_e.asp)

Version 1: February 2015