ICHA | Inner City Health Associates

POLICY TITLE **Privacy breach Protocol**	
APPROVED BY: Operations Director	
DATE APPROVED: April 4, 2019	**Operations Director SIGNATURE:**
DATE REVIEWED/REVISED:	

Inner City Health Associates (ICHA) is the owner and administrator of the OSCAR Electronic Medical Record used by ICHA physicians, staff, and by ICHA partner agencies. ICHA is both a Health Information Custodian (HIC) and a Health Information Network Provider (HINP). Each agency's privacy policies will at a minium 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 suspects unauthorized access following an audit of the ICHA EMR, receives a self report, becomes aware of lost or stolen personal health information 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 (USB) with health information saved on the hard drive is lost or stolen
- A courier package is not delivered to the correct address and opened
- A patient reads another patient's health record on a computer while waiting in a clinic room
- 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 or placed in a secure confidential container.
- Health information is given to the media without consent
- Unauthorized access which includes the viewing of personal health information in electronic information systems, and may be motivated by a number of factors including interpersonal conflicts, curiosity, personal gain or concern about the health and well-being of individuals

Privacy Breach Protocol[1]

The first individual/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

[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

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:

Step 1: 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 and Operations Director.
- The Medical Director in consultation with the Operations Director is responsible for determining if the Board of Directors needs to be informed.
- Determine which agencies are affected and notify them as appropriate,
- As outlined in section 12(3) of PHIPA and its related regulation, plan for the notification of the Information and Privacy Commissioner of Ontario (the Commissioner)
- 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 (as appropriate)

- 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)
- Any breach of unauthorized access will prompt a deactivation of the individual(s) Oscar access, pending further investigation.
- 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.

Step 3: Notification

- Where other HICs are involved, consult with and identify the HIC or HICs that will lead in notification.
- Where a Non-HIC is involved ICHA will take the lead in investigation and notification.
- The Act requires that individuals affected by the breach or their Substitute Decision Makers (SDM) are notified at the first reasonable opportunity.
- Notification will first be discussed by the notifying Privacy Officer and where appropriate 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.
- Notification will include:
    - ✓ The details and extent of the breach;
    - ✓ The specifics of the PHI at issue;
    - ✓ The steps that have been taken/will be taken to address the breach;

- ✓ That the IPC was notified of the breach;
- ✓ The contact information of the person within your organization, if the individual has any further questions?
- ✓ Information on how to complain to the Privacy Commissioner

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, ICHA-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.
- Under section 12(3) of PHIPA and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. These include:
    1. Use or disclosure without authority
    2. Stolen information
    3. Further use or disclosure without authority after a breach
    4. Pattern of similar breaches
    5. Disciplinary action against a college member
    6. Disciplinary action against a non-college member and
    7. Significant breach
- Where an employee is a member of a college, you must notify the College of the privacy breach if:
    - you terminate, suspend or discipline them as a result of the breach
    - they resign and you believe this action is related to the breach
- Where a health care practitioner with privileges or otherwise affiliated with you is a member of a college, you must notify the Commissioner of a privacy breach if:
    - you revoke, suspend or restrict their privileges or affiliation as a result of the breach
    - they relinquish or voluntarily restrict privileges or affiliation and you believe this action is related to the breach

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)

Reporting a Breach to the Commissioner

(https://www.ipc.on.ca/wp-content/uploads/2017/08/health-privacy-breach-notification-guidelines.pdf)

Privacy Breach Protocol

(https://www.ipc.on.ca/health/breach-reporting-2/privacy-breach-protocol/)

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)

Draft September 2018