April 2017

Hamilton Family Health Team

Privacy Breach Protocol[1]

This is part of the Hamilton Family Health Team Privacy Policy.

Report

All privacy breaches must be reported immediately to the Executive Director of the Hamilton Family Health Team from the applicable Family Health Organization who act as the Privacy Officers.

If a privacy breach happens within an individual family physician's office and it can be addressed there, then it should be and also should be reported to the relevant FHO's lead physician. If a privacy breach cannot be managed within the family physician's office, the Privacy Officers can be contacted to assist.

Annually each FHO will submit a report to the Privacy Officers who will make a full report to the board of the Hamilton Family Health Team.

Privacy Breach

A privacy breach happens whenever a person contravenes or is about to contravene a rule under the *Personal Health Information Protection Act, 2004* (PHIPA) or our privacy policies. The most obvious privacy breaches happen when patient information is lost, stolen or accessed by someone without authorization.

For example:

- An unencrypted laptop with health information saved on the hard drive is stolen
- A courier package of patient records is not delivered to the correct address
- An unencrypted USB key with an Excel spreadsheet with patient information or Word files is lost
- A patient reads another patient's health record on a computer while waiting in a clinic room
- A Team Member talks about a patient with a friend
- Team Member sends an email to a "help desk" attaching a worksheet with patient information but does not check the email address and instead of sending the attachment internally – sends it to the last help desk emailed which is at a bank
- Health records to be disposed of are recycled and not shredded
- Out of curiosity, a Team Member reviews a neighbour's health record
- A student or any other Team Member looks at health records of patients on a self-initiated education project without being assigned to those patients and without specific authorization for an approved educational exercise
- Health information is given to the media

[1] Based on the Information and Privacy Commissioner/Ontario "Privacy Breach Protocol". Available online: https://www.ipc.on.ca/health/breach-reporting-2/privacy-breach-protocol/.

- A Team Member makes a copy of an ex-spouse's health record without it being part of the Team Member's position to do so
- Team Members discuss patients in hallways and lunchrooms and other patients overhear (even colleagues overhear)
- Team Member releases information to another health care provider when a patient has said she doesn't want that provider to know
- Team Member releases information to a spouse when the patient doesn't want that spouse to know
- Team Member releases information to a child's parent when the child is capable of making his own decisions and said don't tell my parents

Privacy Breach Protocol

The following steps will be taken by the Privacy Officers (or delegate) if they believe there has been a privacy breach:

Step 1: Respond immediately by implementing the privacy breach protocol

- Ensure appropriate staff members within the Hamilton Family Health Team and the applicable Family Health Organization are immediately notified of the breach, including the Privacy Officers and the physicians whose patients are potentially affected by the privacy breach.

- Address the priorities of containment and notification as set out in the following steps.

- Consider engaging legal counsel or a privacy breach coach if appropriate.

- Consider notifying the Information and Privacy Commissioner/Ontario (IPC/O) (www.ipc.on.ca) As time passes, the Privacy Officers will revisit this need to report on an ongoing basis. It may be premature to report if unclear whether there has been a breach or if unclear of the scope of the breach. The Privacy Officers may need to keep the IPC/O apprised through this process.

- Consider when to notify the insurer (which may be a condition of coverage), senior management, the Board Chair, and other key internal stakeholders.

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

- Retrieve and secure any personal information that has been disclosed or inappropriately used or collected (including all electronic or hard copies). This might include attending at the scene to determine whether there are any other records in public.

- Ensure that no copies of personal health information have been made or retained by the individual who was not authorized to collect, use or receive the information. Obtain the 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. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords or identification numbers, temporarily shut down a system, suspend an individual or group's access to the system, implement security, institute a lockbox or restriction to the file).

- Consider notifying or updating the IPC/O and/or legal counsel if appropriate.

Step 3: Clarify the facts

- Consider whether there is sufficient expertise to conduct an internal investigation or whether a specialist (such as an IT security specialist) is required

- Determine the scope of the breach:
    - Details of the incident and how it was discovered
    - Number of people affected
    - Who was involved
    - Dates
    - Type of incident (such as:)
        - Unauthorized use
        - Unauthorized disclosure
        - Hacking, malware, security breach
        - Lost/stolen mobile device
        - Lost/stolen hard copies
        - Refused access or correction request
        - Fax to wrong number
        - Email to wrong recipient

- Determine how it happened and who was involved and why

Step 4: Notification - Identify those individuals whose privacy was breached and notify them of the breach

- At the first reasonable opportunity, any affected patients (or others whose personal health information has been affected) will be notified. Give careful consideration to whether affected individuals need to know immediately (especially were despite efforts, the breach is ongoing or where the information in question is of a highly sensitive nature or there is reason to believe that it will be used in a malicious way)

- The type of notification will be determined based on the circumstances (such as the sensitivity of the personal health information, the number of people affected, and the potential effect the notification will have on the patient(s)).

    - For example, notification may be by telephone or in writing, or depending on the circumstances, a notation made in the patient's file to be discussed at his/her next appointment.

    - In some cases, a public notice is the most efficient and effective method of notice.
    - Focus on considerations such as:
        - The potential privacy impact of calling the individual's home or sending a letter
        - Whether the affected individual will be coming in to see a health care provider very soon and could be told in person

        - Whether anyone affected is in a vulnerable state of health or deceased or a child or incapable to make information decisions such that notice would be given to a substitute decision-maker and consider the best way to manage those sensitive issues

- 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.
- Establish a plan to address what clinical and administrative staff and others should do if they receive calls about the privacy breach.
- Consider notifying the IPC/O and/or legal counsel if appropriate – especially if required by law.

Step 4: Investigation and Remediation

- Conduct an internal investigation into the matter. The objectives of the investigation will be to:
    - Ensure the immediate requirements of containment and notification have been addressed.
    - Review the circumstances surrounding the breach.
    - Review the adequacy of existing policies and procedures in protecting personal health information.
    - Address the situation on a systemic basis.
    - Identify opportunities to prevent a similar breach from happening in the future.
- Change practices as necessary.
- Ensure staff are appropriately re-educated and re-trained with respect to compliance with the privacy protection provisions of PHIPA and the circumstances of the breach and the recommendations of how to avoid it in the future.
- Continue notification obligations to affected individuals as appropriate.
- Consider notifying the IPC/O and/or legal counsel as appropriate.
- Consider any disciplinary consequences with staff or contract issues with independent contractors or vendors that follow from the privacy breach.

Additional Notes about Specific Kinds of Breaches:

Fax: Clinicians should use their judgment when it comes to implementing this Privacy Breach Protocol as a result of a misdirected fax. For single instances of a fax that is misdirected to another health care provider, ensuring that the recipient securely destroyed the fax may be sufficient. Clinicians may choose to put a reminder in the chart to discuss the breach (and actions taken to correct it) next time the patient visit the clinic. Clinicians should be aware that they may face increased consequences if they do not implement the full Privacy Breach Protocol whenever a breach occurs. Please report all stray faxes to your Privacy Officer. And situations where there are repeated stray faxes must be reported to the Privacy Officers to assess whether a report to the Information and Privacy Commissioner is required and how to notify affected individuals.

Misfiled records: When patient information is filed in the wrong health record, it should be corrected immediately. It may be appropriate to choose *not* to enact this Privacy Breach Protocol when a test result is filed in the wrong chart, if a clinician feels confident that the misfiled information was not accessed by another healthcare provider to make healthcare decisions on behalf of the patient, and that no other patient would have had access to the information (for example, through a request for a copy of the chart). If it is possible that the information could have been used to make treatment decisions or could have been shared with an unauthorized third party, then the Privacy Breach Protocol should be enacted.