285 Sarah Avenue North
Listowel, ON N4W 2Y8
T: (519) 291-3125
F: (519) 291-6028

BOARD POLICY

Subject:	Breach of Privacy of Personal Health Information	Date Approved:	September 25, 2008
Approved by:	Board of Directors	Date Revised:	March 22, 2010
Specific to:	All Staff, Board of Directors	Next Review Date:	January 2012

POLICY

The North Perth Family Health Team (NPFHT) as a Health Information Custodian (HIC) under the Personal Health Information Protection Act (PHIPA) 2004 is responsible and accountable for the privacy and security of the personal health information (PHI) under its custody and control.

It is the policy of NPFHT that all employees and affiliates will:

- comply with obligations related to privacy and confidentiality
- protect and secure all personal health information (PHI) entrusted to them, to prevent a breach of a patient's privacy
- to act immediately if made aware of an actual or potential privacy breach.
- Participate in the investigation and management of a privacy breach with appropriate representation, as applicable.

A privacy breach occurs whenever:

- PHI is lost or stolen, or
- PHI is accessed, disclosed, copied or modified without authority, or
- Disposal of PHI has occurred in an insecure manner,or
- Any other situation where an employee, or affiliate has contravened, or is about to contravene the Personal Health Information Protection Act (PHIPA) 2004

A privacy breach can occur via verbal or written communication, via phone, e-mail, fax or any other medium.

A privacy breach can be actual, or potential. (see definitions of actual, or potential privacy breaches for examples).

Pursuant to (PHIPA 2004), NPFHT must notify a patient, or the patient's Substitute Decision Maker (SDM), if there has been a breach of privacy related to their PHI. It is the responsibility of the Privacy Officer or delegate to notify the patient or SDM. (Note: the Privacy Officer is the Executive Director)

A breach of privacy may be cause for disciplinary action up to and including termination of employment/contract or loss of appointment or affiliation with the organization as outlined in the Privacy Policy, Confidentiality Policy and the Privacy and Confidentiality Agreement signed by all employees and affiliates.

PROCEDURE

NPFHT may become aware of a potential or actual privacy breach by:

285 Sarah Avenue North
Listowel, ON N4W 2Y8
T: (519) 291-3125
F: (519) 291-6028

- Patients, employees or affiliates who believe personal health information has been breached or compromised may complain to the caregiver or the Privacy Officer or delegate,
- A representative from the IPC will notify the Privacy Officer or delegate and request a response within a specified period of time, following a patient complaint to the IPC.
- An audit of the organization's electronic medical record system (EMR) or other system containing personal health information has resulted in reason to believe that there may have been an inappropriate access to a patient's personal health information,
- Health Information Custodians(HIC), private homes, businesses or individuals who are not health care providers reporting a potential or actual breach to the Privacy Officer or delegate or their Leader or delegate.
- A secondary breach identified through the initial investigation of another breach.

In accordance with guidelines provided by the Office of the Information and Privacy Commissioner of Ontario, NPFHT will take the following steps when made aware of a potential or actual privacy breach.

Step 1: Act Immediately: Contain the Breach and Secure the Personal Health Information

Employees and affiliates, upon learning of a potential or actual privacy breach must notify the Privacy Officer or delegate, immediately.

Depending on the severity and nature/type of the breach:

- The Privacy Officer or delegate may involve the following individuals as soon as reasonably possible,
    - Board Chair
    - Medical Director
    - Information Management, and/or the Trusted User (if immediate suspension of access is required to further contain the breach)
    - Police if the breach may reasonably be considered to result in significant harm to the patient or third party.
    - Others as deemed necessary.

- The Privacy Officer or delegate will direct employees and affiliates to immediately contain the breach.
  Containing the breach may include:
    - Determining whether the breach would allow unauthorized access to any other personal health information and, if so, take any and all steps necessary to contain the breach, e.g. change passwords, or temporarily shut down a system,
    - Suspending a users' access to patient care systems or other hospital systems to prevent reoccurrence of the breach. Suspending a user's access will only be done with the authority of Executive Director or designate.
    - Notifying the employee(s) involved of the situation, indicating that an investigation is being conducted, and that the Privacy Officer or delegate will be monitoring their access.
    - In the case of information that has been mailed or faxed to the wrong recipient retrieving the information by:

285 Sarah Avenue North
Listowel, ON N4W 2Y8
T: (519) 291-3125
F: (519) 291-6028

- obtaining contact information from the recipient,
- asking the recipient to place the information in a sealed envelope and place in a secure area,
- asking the recipient not to make any copies of the information,
- notify the Privacy Officer or delegate who will arrange a courier to retrieve the information, if required.

Step 2 Investigate the Potential/Actual Breach and Evaluate the Risks Associated with the Breach

The Privacy Officer or delegate will conduct an investigation to determine the extent of the breach. Steps that may be taken as part of the investigation include:

- auditing the electronic patient record (EPR),
- hard copy health record review,
- interviews with employees, Physicians, students, volunteers, or affiliates,
- interviews with patients and or SDM.

Depending on the severity of the breach, the Privacy Officer or delegate will identify and manage risks associated with the breach, including risk related to:

- reputation of the organization
- patient trust
- media
- legal
- collaborate on determining next steps/actions

Outcomes for employee/affiliate:

On completion of the investigation, the Privacy Officer, in collaboration with the Board Chair and Medical Director determines the most appropriate outcome for the employee/affiliate. Possible outcomes include one or more of the following:

- Education
- Verbal warning
- Written warning
- Suspension
- Termination

Factors to consider when determining an outcome include:

- history of work performance or any prior discipline. Note the time lapse between disciplinary infractions and the employee's tendency to respond favourably to discipline
- years of service
- employee/affiliate’s response to investigation
- whether the employee/affiliate understands the concept of privacy and confidentiality and understands the seriousness of the breach

285 Sarah Avenue North
Listowel, ON N4W 2Y8
T: (519) 291-3125
F: (519) 291-6028

North Perth Family Health Team
Helping you to health yourself

Step 3 Notification

Patient Notification

The Privacy Officer are legally required to notify;

- a patient or an incapable patient's Substitute Decision Maker (SDM), if the patient's information has been lost, stolen or accessed without authority

Notification of a patient/SDM may be done verbally or in writing depending on several factors:

- availability of the patient/SDM, i.e. if the patient is coming to the medical clinic in the near future, it may be appropriate for the physician or Privacy Officer to notify the patient in person,
- relationship with the patient i.e. if the physician or leader has an established clinical relationship with the patient, it may be appropriate to notify the patient in person.

When applicable, the notification indicates that an employee has received disciplinary action but does not disclose details of the action, e.g. that the staff received a written warning or a suspension. The initial notification does not disclose the name of the employee who committed the breach, but if the patient requests this information, this information is disclosed.

Other Organizations

In the event that an actual, or potential breach is identified as involving or potentially involving another organization's employee/user and/or a patient's Personal Health Information, through the electronic medical record (EMR) or other communication venues, the Privacy officer will immediately:

- Notify the Privacy Officer, or designate of the organization(s) that are affected by the breach.

The Office of the Privacy Commission of Ontario (IPC)

Depending on the severity of the breach, the Privacy Officer or delegate is responsible to submit a report outlining the breach, the investigation, patient notification and outcome to the Office of the Information Privacy Commissioner of Ontario and work with the Commissioner's staff to ensure the organization has met its legal obligations under PHIPA.

Step 4 Managing the Risk of Future Breaches

Depending on the severity of the breach, those involved in managing the breach will review the breach and information obtained as part of the investigation with an aim to take measures to reduce the risk of reoccurrence. These measures may include:

- changes to processes, policies or procedures,
- additional education and training for employees and/or affiliates related to personal health information and their accountabilities for confidentiality and the protection of patients privacy rights,
- reviewing and enhancing the programs or department's security of personal health information

DEFINITIONS

Health Information Custodian: Listed persons or organizations under the Personal Health Information Protection Act such as hospitals and physicians, who have custody or control of personal health information as a result of the work they do.

285 Sarah Avenue North
Listowel, ON N4W 2Y8
T: (519) 291-3125
F: (519) 291-6028

Affiliates - Individuals who are not employed by the organization but perform specific tasks at or for the organization, including appointed professionals (e.g., physicians/midwives/dentists), students, volunteers, researchers, contractors, or contractor employees who may be members of a third-party contract or under direct contract to the organization, and individuals working at the organization, but funded though an external source.

Personal health information is any identifying information with respect to an individual, whether living or deceased and includes:

- Information concerning the physical or mental health of the individual;
- Information concerning any health service provided to the individual;
- Information concerning the donation by the individual of any body part or any bodily substance of the individual;
- Information derived from the testing or examination of a body part or bodily substance of the individual;
- Information that is collected in the course of providing health services to the individual; or
- Information that is collected incidentally to the provision of health services to the individual.

Privacy Breach – Actual - includes, but is not limited to:

(a) accessing patient personal health information when it is not required to provide or maintain care to a patient or in the performance of duties, for example:

- Directly accessing the electronic health record of one self without following Health Record Services procedure.
- Accessing the health record of an employee, family member, friend, or anyone for whom you do not have a requirement to view information based on providing care or performing duties
- Accessing any patient information (e.g. address, date of birth, next of kin, etc.) of an employee, family member, friend, or anyone for whom you do not have a requirement to view information based on providing health care or performing duties.

(b) Discussing patient information with:

- Another person who is not involved in the direct care of the patient or does not require the information to perform their job functions, or
- Within range of other people in a non-patient care area of the hospital. (For example: discussing information related to patient care with another employee in the waiting area.)

(c) Failing to ensure the security of patients' PHI, for example:

- faxing or e-mailing PHI to the wrong recipient,
- theft of electronic devices containing identifiable patient information

Privacy Breach – Potential – occurs when an individual's personal health information is at high risk of being accessed, used or disclosed inappropriately by or to individuals or for purposes other than consented to by the patient. A potential privacy breach includes, but is not limited to:

- allegations of a privacy breach by a patient or employee/affiliate
- concerns related to security of PHI raised by a patient or employee/affiliate
- request by a patient for additional security around their PHI (e.g. Lock Box).

285 Sarah Avenue North
Listowel, ON N4W 2Y8
T: (519) 291-3125
F: (519) 291-6028

- leaving patient information in unattended or unsecured locations where it may be accessed by unauthorised persons.
- leaving access to electronic patient information unattended on an open log in,
- storing electronic patient identifiable information on portable information devices or un-secure drives, e.g. hard drives that have not been encrypted
- loss of a hard copy health record or other identifiable patient information

Substitute Decision Maker (SDM) is defined as a person who is:

- at least 16 years of age, unless he or she is the incapable patient's parent,
- capable with respect to the treatment,
- not prohibited by court order or separation agreement from having access to the incapable patient or giving or refusing consent on the incapable patient's behalf,
- available; and
- willing to assume the responsibility of giving or refusing consent.

In descending order of priority, an incapable patient's SDM may be:

i. the incapable patient's **"guardian of the person"**, appointed under the Substitute Decisions Act, 1992, if the guardian has authority to give or refuse consent to the treatment,
ii. The incapable patient's **"attorney for personal care"**, given under the Substitute Decisions Act, 1992, if the power of attorney confers authority to give or refuse consent to treatment
iii. the incapable patient's **"representative"** appointed by the Consent and Capacity Board, if the representative has authority to give or refuse consent to the treatment
iv. the incapable patient's **spouse** or **partner**
v. a **child or parent (custodial)** of the incapable patient, or a Children's Aid Society or other person who is lawfully entitled to give or refuse consent to the treatment in the place of the parent
vi. a **parent (who has only a right of access)** of the incapable patient
vii. a **brother or sister** of the incapable patient
viii. **any other relative** of the incapable patient
ix. the **Public Guardian and Trustee**

REFERENCES

Legislation and Other Resources:

Personal Health Information Protection Act, 2004 (http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm)

Regulated Health Professions Act 1991 (as amended) (http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/91r18_e.htm)

Standards:

285 Sarah Avenue North
Listowel, ON N4W 2Y8
T: (519) 291-3125
F: (519) 291-6028

[College of Nurses of Ontario, Standards of Practice – Confidentiality and Privacy - Personal Health Information]

[College of Physicians and Surgeons of Ontario – Confidentiality and Access to Patient Information]