INFORMATION PRACTICES:

ELECTRONIC HEALTH RECORD AND ELECTRONIC INFORMATION SYSTEMS

While the provisions of the *Personal Health Information Act* (*PHIA)* apply to both paper and electronic information, this section focuses on factors around personal health information in an electronic format. It reviews the requirements in the *Act* and its regulations as they relate to electronic health information and provides guidelines around information practices that custodians can put in place to ensure compliance with the legislation.

DEFINITIONS

ELECTRONIC HEALTH RECORD

An Electronic Health Record (EHR) as defined in the regulations means *"an electronic information system that is approved by the Minister and integrates data from multiple electronic information systems for the purpose of providing a comprehensive record of an individual's personal health information*." (*PHIA* regulation section 2(1))

Examples of an electronic health record for Nova Scotia include the Secure Health Access Record (SHARE) and, once implemented, the Nova Scotia Drug Information System (DIS).

ELECTRONIC INFORMATION SYSTEM

An Electronic Information System is defined in regulation as "*a computer system that generates, sends, receives, stores or otherwise processes personal health information*" (*PHIA* regulation section 2(2)). Many custodians use electronic information systems in documenting the treatment and/or scheduling of individuals under their care.

An example of an electronic information system would be the Nightingale™ system, an electronic medical record used by many physicians in their practices, as well as the Nova Scotia Hospital Information System (NShIS). An electronic information system can also be a single computer which tracks appointments, billings or a patient's personal health information in a sole practitioner's office.

OVERVIEW

PHIA requires that custodians implement, maintain and comply with information practices for both paper and electronic information that:

(a) meet the requirements of the Act and the regulations;
(b) are reasonable in the circumstances; and
(c) ensure that personal health information in the custodian's custody or under its control is protected against
   a. theft or loss of the information, and
   b. *unauthorized access to or use, disclosure, copying or modification of the information.* (*PHIA* section 62)

INFORMATION PRACTICES IN AN ELECTRONIC ENVIRONMENT

Under *PHIA* regulations, custodians must implement additional safeguards for personal health information held in an electronic information system maintained by the custodian as outlined:

(a) protection of network infrastructure, including physical and wireless networks, to ensure secure access;

(b) protection of hardware and its supporting operating systems to ensure that the system functions consistently and only those authorized to access the system have access;

(c) protection of the system's software, including the way it authenticates a user's identity before allowing access. (*PHIA* regulation section 10 (1))

In addition, a "*custodian must create and maintain written policies to support and enforce the implementation of the safeguards…*" (*PHIA* regulation section 10 (2)).

Ensuring that personal health information is protected requires the successful integration of three types of security measures:

- administrative safeguards;
- physical safeguards; and
- technical safeguards.

Administrative safeguards, along with physical and technical safeguards are the technologies, policies and procedures that protect personal health information and control access to it.

PHIA requires that custodians take steps, appropriate to their organization, to protect the personal health information that is under their custody or control. Custodians may choose to conduct a risk assessment of all their electronic information systems to evaluate the potential risks and vulnerabilities to the privacy, confidentiality and integrity of the personal health information. Once conducted, custodians can then consider how best to implement the administrative, physical, and technical safeguards necessary to adequately protect the personal health information. Factors to consider may include the sensitivity of the information, the risks associated with exposure of the information, the size of the organization or of the electronic system itself as well as the number of users of the system.

EXAMPLE

Louise is the Chief Information Officer of a District Health Authority with hundreds of electronic information systems holding thousands of patient records, along with thousands of potential users. Louise may consider purchasing an advanced audit system able to accept feeds from the many systems and produce audit reports to ensure that the systems are being accessed appropriately.

In contrast, Louise’s brother, Andrew, is a physician in his own practice with one additional employee, his receptionist. He may choose to use strong password protection and lock his office whenever he steps out to prevent anyone else accessing his patients’ information as part of his information safeguards.

ADMINISTRATIVE SAFEGUARDS

According to the Treasury Board of Canada, administrative safeguards are "*the written policies, directives, rules, procedures and processes for the protection of personal information throughout the life cycle of both the personal information and the program or activity*."[1]

Administrative safeguards may include the establishment of appropriate security policies, procedures and practices, supported by adequate training and education of staff, and appropriate enforcement. The following are some examples, including those that are required under *PHIA*

- appointment of a privacy officer/*PHIA* contact person (*PHIA* section 67*)*
- written security policies/guidelines (*PHIA* regulation section 10(2))
- written privacy statement (*PHIA* section 15*)* [2]
- staff privacy and confidentiality training to maintain awareness of policies and guidelines;
- audits (including an audit schedule) for compliance with security policies;
- confidentiality agreements for employees and agents; and
- contracts with agents that ensure compliance with the *Act* and regulations.

The most robust physical and technical safeguards can be compromised if the custodian's agents, including employees, consultants and volunteers are not aware of proper information practices - or if they disregard them. Breaches of personal health information held electronically are most likely to be committed by authorized users of the systems, who therefore pose the greatest risk. [3] Regular updating of the policies and guidelines and a schedule for regular training may help mitigate that risk.

[1] Treasury Board of Canada Secretariat. Directive on Privacy Practices. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=18309#appA

[2] See Chapter 3: *Duties of a Custodian* and Template 3-4 *Written Privacy Statement*

[3] Veriphry: Survey of Patient Privacy Breaches, August 2011. http://blog.veriphyr.com/2011/08/over-70-of-healthcare-providers.html

PHYSICAL SAFEGUARDS

Physical safeguards are designed to protect both your system and the personal health information stored on it from unauthorized use, loss or damage. When assessing and implementing physical safeguards, custodians should consider the risks associated with *all* access to personal health information which may include access within the facility, but also all other physical locations where it may be accessed or stored.

Physical safeguards may include:

- Establishing secure areas and using identity badges in secure areas (where required and feasible).
- Maintaining access records for individuals who have access to secure areas. The access records should be meaningful in the event of a security audit.
- Ensuring that appropriate security mechanisms are used at any unattended entrance to a secure area (e.g. locks on doors, card access control, monitored surveillance cameras).
- Placing monitors, printers and fax machines where others cannot see personal health information (e.g. away from waiting rooms, ground floor windows or busy passageways).
- Ensuring equipment is kept in a locked office whenever you are out of the office or away for extended periods of time (e.g. overnight, vacation).
- Keeping portable equipment secure (e.g. do not leave laptops in your vehicle).
- Keeping USB memory devices, CDs, and other media in a secure place (e.g. a locked drawer).
- Maintaining the ability to quickly restore critical systems in the event of equipment loss or failure.
- Disposing of all media containing sensitive information in a secure manner, which includes shredding, disintegration and incineration.[4]

[4] COACH*: Putting it in Practice: Privacy and Security for Health care Providers Implementing Electronic Records* http://www.ehealthontario.on.ca/images/uploads/pages/documents/Putting-it-into-Practice_PrivacySecurityHealthcareProviders.pdf

TECHNICAL SAFEGUARDS

Technical safeguards protect the personal health information in computer systems, networks and other information resources. Implementation of technical safeguards and standards represent good business practices to protect the personal health information under a custodian's custody or control.

a) Measures to protect network infrastructure

Custodians should review their network's protection against unauthorized access to protect network infrastructure from external (e.g. malware and hackers) and internal threats (e.g. network operational centres should be kept locked).

EXAMPLE

At the Northeast Grace Hospital the firewall prevents users from accessing certain high risk websites to minimize the risk of hackers. Melissa, a registration clerk at the hospital, logs on to the system at work and wants to check her horoscope. She receives a message stating that she is not allowed to access this website.

b) Measures to protect hardware/operating systems

Various measures can be utilized to protect hardware and their supporting operating systems to ensure security by avoiding unauthorized access. For example, back-up information should be stored in a secure, locked environment off-site. Information intended for long-term storage on electronic media should be reviewed on a regular basis to ensure the data is retrievable, and to migrate the data to another storage medium if necessary.

c) Measures to protect a system's software and data

There are a number of measures that can be used to protect a system's software:

- Disaster recovery models can be implemented by having up-to-date backups of all data securely stored in a location other than where the data is normally stored.
- Encryption and authentication minimizes the risk of access by unauthorized individuals.

  - Encryption or cryptography is the general term for mechanisms to convert data for secure transmission or storage.
  - Authentication is any process that verifies the source of a request or response for information in a computing environment. Authentication can be based on one or more of the following criteria:
    1. something you have – e.g. a key, card
    2. something you know – e.g. password, personal I.D. number
    3. something related to who you are – e.g. signature, iris pattern, voiceprint, thumb print
    4. something indicating where you are located – e.g. terminal connected by hardwired line, phone number
- Antivirus/antimalware software can protect against unauthorized modification, loss, access, or disclosure. As viruses and malware threats are constantly changing and advancing, it is important to ensure antivirus/antimalware software is up-to-date to protect from such threats.
- Internet access should be through a firewall implemented through hardware (e.g. on a network router) or software residing on the user machine.
- Particular attention is required to protect data during transport or on a mobile device. There are different considerations that should be taken into account to ensure the security of the data.
  - Devices such as laptops, memory sticks and smart phones may facilitate mobility; however these devices should only be utilized for personal health information if the appropriate security measures are in place.
  - Encryption may mitigate the risk of transporting data and it is recommended that, when taking data from a secure office location and putting it onto a mobile device or transporting it otherwise, data should be encrypted.
- Security is also dependent on the person not sharing their access directly or indirectly, through careless storage of user IDs and passwords. For example post-it notes on monitors can lead to unauthorized access. Another element of security is restricting access to personal health information by staff on a need-to-know basis; only those who need to have access to the personal health information for the purpose of carrying out their job functions should have access.

SECURITY AND PRIVACY BREACHES

The *PHIA* regulations state that:

"A custodian shall create and maintain a record of every security breach of the custodian's electronic information system that the custodian determines on a reasonable basis is likely to pose a risk to an individual's personal health information. (*PHIA* regulation section 10 (3))

A record of security breaches must include details of all corrective procedures taken by the custodian to diminish the likelihood of future security breaches." (*PHIA* regulation section 10 (4))

Security breaches that pose a risk to personal health information should be thoroughly documented and analyzed to determine the root cause or causes of the breach. Once the root cause has been identified, corrective action is required to minimize the risk of the event happening in the future. The effectiveness of the corrective measures as a mitigation strategy should also be evaluated over time as part of a continuous improvement cycle.

Information regarding privacy breaches can be found in Chapter 3 of the Toolkit, *Duties of a Custodian*.

RECORD OF USER ACTIVITY

In subsection 63(3) of the *Act*, a "*record of user activity related to an individual's personal health information*" means a report produced at the request of an individual for a list of users who accessed the individual's personal health information on an electronic information system for a time period specified by the individual. (*PHIA* regulation section 11(1))

Section 63 of *PHIA* gives individuals the right to request a record of user activity for any electronic information system that a custodian uses to maintain the individual's personal health information. The record of user activity may be generated manually or electronically. It is important to note that the record of user activity must be made available within 30 days and at no charge.

The *PHIA* regulation section 11 (2) provides that the record of user activity *"…must include at least all of the following information:*

> *(a) the name of the individual whose personal health information was accessed;*
>
> *(b) a unique identification number for the individual whose personal health information was accessed, including their health-card number or a number assigned by the custodian to uniquely identify the individual;*
>
> *(c) the name of the person who accessed the personal health information;*
>
> *(d) any additional identification of the person who accessed the personal health information, including an electronic information system user identification name or number;*
>
> *(e) a description of the personal health information accessed or, if the specific personal health information accessed cannot be determined, all possible personal health information that could have been accessed;*
>
> *(f) the date and time the personal health information was accessed or, if specific dates and times cannot be determined, a range of dates when the information could have been accessed by the person.*

As per *PHIA* regulation 11(2), a custodian must be able to capture at least the above information within the record of user activity. Given that not all custodians have (or should have) an elaborate electronic information system with robust audit functionality, the regulation allows for a broad response to the specific type of personal health information accessed along with ranges for the dates and times.

Therefore, custodians unable to extract this information electronically from their electronic information system are still able to comply with the regulation by providing a more general description. This information may be captured through the custodians scheduling system (date and time) along with a detailed list of the personal health information captured by the applicable system.

EXAMPLE

Herbert is a naturopathic doctor operating a clinic with two support staff, an electronic scheduling system, and paper records. Eileen, a patient of the clinic, requests a record of user activity. Herbert explains to Eileen that his system is not able to produce a record detailing the specific times of access and by whom, but based on his hours of operation, and having only two staff members – he gives Eileen a record of user activity highlighting the following information:

- Herbert and his two staff members (Shirley and Tina) may have accessed Eileen's personal health information contained in the electronic system (demographics, medical conditions, allergies) at any point during the clinic's hours of operation (Monday – Friday, 8 a.m.-5p.m.) during the past six months.
- Both staff members have legitimate work reasons to access the personal health information for scheduling appropriate appointment times and for filing any follow-up test results.

AUDIT LOG VERSUS RECORD OF USER ACTIVITY

Individuals should be made aware that under *PHIA* they have the right to request a record of user activity that shows who has looked at their personal health information in an electronic format. Information about this right could be included in the custodian's privacy statement.

It is important to distinguish between an "audit log" and a "record of user activity" referenced in section 63 of *PHIA*:

> A record of user activity "*means a report produced at the request of an individual for a list of users who access the individual's personal health information on an electronic information system for a time period specified by the individual*" (*PHIA* regulation section 11 (1)).
>
> An audit log, if one exists, is an electronic file or record which details, during a given period of time, who has accessed patient information in an electronic information system. The audit log may or may not contain more fields than those required by regulation to produce a record of user activity.

A record of user activity may be generated by taking specific fields from a system's audit log and forming a report that could be provided to an individual. The *PHIA* regulations require that the audit logs used to generate a record of user activity, if they exist, must be kept for at least one year from the date they were used to create a record of user activity (*PHIA* regulation section 10(2)). A custodian will determine the retention period for the audit logs on an ongoing basis and this can be included in their written policies.

EXAMPLE

Nadine is the Privacy Manager at a hospital that has purchased an advanced audit system capable of producing audit reports to ensure that systems are being accessed appropriately. Norman, a previous patient at one of the hospitals, requests a record of user activity. He is concerned that his neighbour, who is a nurse at the hospital, may have looked at his personal health information.

Nadine is able to produce a record of user activity from the audit logs it runs on a monthly basis and retains for a three year period (as outlined in their policy). The hospital will be required to keep all audit logs used to produce the record of user activity for one year from the date his record of user activity was created.

Custodians may also consider capturing the following elements in their audit logs:

- the location of the user when the information was accessed;
- the specific action performed or conducted by the user (e.g. viewing, modifying, deleting, printing, editing, signing off, writing); and
- the length of time the action took place.

SECURE DESTRUCTION

Under section 49(2) of *PHIA*, retention schedules require that information no longer required to fulfill the purposes identified in the schedules (e.g. direct patient care) be securely destroyed, erased or de-identified.

Section 49 (1) of *PHIA* states that "securely destroyed" means destroyed in such a manner that reconstruction is not reasonably foreseeable.

It is important to be aware that physically destroying hardware and patient information records in an electronic form can be difficult. Secure destruction of electronic records requires professional expertise. There are four main options described below for secure destruction of personal health information held electronically:

1. Wiping Hard Drives
Data-wiping software is available to wipe hard drives previously used in your practice or clinic.

2. Degaussing Hard Drives
Degaussing uses a reverse magnetic field to scramble electronic data in a hard drive and make stored information unreadable.

3. Secure Erase
Secure erase permanently removes information from a hard drive by prompting a pre-existing protocol coded into the hard drive by the manufacturer.

4. Physical Destruction
Physical destruction of a hard drive means to physically destroy in an irreversible manner so that the record(s) cannot be reconstructed in any way.[5]

Please note that "regular" deletion of files is not adequate (including any "Empty Trash" feature) - the data may still exist on the media. Given the technological expertise to securely destroy electronically stored information, consideration should be given to hiring an accredited service provider when destroying personal health information.

Acceptable methods of secure destruction for electronic records containing personal health information will evolve over time. It should be recognized that these approaches are separate from the ultimate destruction of the hardware itself (e.g. to securely remove the information at the end of life cycle of the hardware).

[5] Alberta Netcare (Physician Office System Program) Hardware and Information Disposal.
www.posp.ca/media/307163/hardware_destruction.pdf