Physician Privacy Training

Published:
February 2015

Alberta
Netcare
ELECTRONIC HEALTH RECORD

Table of Contents

Important Contacts

Stakeholders and Authorities	For Assistance With
Alberta Netcare www.albertanetcare.ca 1.855.643.8649	Alberta Electronic Health Record (Alberta Netcare) eHealth Support Team: enrolment, use, support security and privacy
Health Information Act (HIA) Help Desk 780.427.8089	HIA compliance, questions specific to Alberta Netcare or Alberta Health as Information Manager of Netcare
Office of the Information and Privacy Commissioner of Alberta www.oipc.ab.ca 1.888.878.4044	PIA submission and review, HIA compliance and privacy incident investigations
College of Physicians & Surgeons of Alberta www.cpsa.ab.ca 1.800.561.3899	Privacy issues involving physicians, ownership of patient records or patient records retention

1. Physician Privacy Training

Introduction

"As a physician, you probably agree that the most important relationship in your professional life is the one you have with your patients. That relationship functions because you serve as steward of the health information entrusted to you by the patient in the privacy of the examining room. Take steps today to be sure you and your staff are doing everything you can to protect that information."

February 17, 2003
Alberta Medical Association,
College of Physicians & Surgeons of Alberta
and the Physician Office System Program

Research shows that when you take privacy rights seriously in your practice, you establish an atmosphere of trust that keeps patients loyal and attracts the best employees. When you establish a comprehensive privacy policy that patients and employees can understand, you are also less likely to become involved in a privacy dispute. Furthermore, under the Health Information Act (HIA), you are required to have privacy and security policies and procedures in place in your clinic.

The purpose of this tutorial is to provide a resource for physicians to ensure their privacy and security knowledge is up to date and in accordance with Alberta's HIA.

Learning Objectives:

At the completion of this tutorial, participants should be able to:

- Summarize the principles behind the regulations in Alberta to safeguard health information in a clinic setting.
- Identify the practical steps custodians should be taking, as stewards of the health information entrusted to them, including policies and procedures that must be in place to safeguard health information in a clinic setting.

Many helpful resource links are provided throughout this tutorial. It is suggested you create a folder to store these links in your web browser when you begin this tutorial so you may refer to them as needed in the future.

IMPORTANT NOTE: This training is not exhaustive. Physicians and clinic staff should refer to the HIA, Health Information Regulation, the Health Information Act Guidelines and Practices Manual, the Canadian Medical Association (CMA) Code of Ethics, and the College of Physicians and Surgeons of Alberta (CPSA) Health Professionals Act Standard of Practice. Additional resources on privacy and security requirements are available through the Alberta Medical Association (AMA) and the CMA.

Physicians are encouraged to make use of other privacy training they may have access to through Alberta Netcare or Alberta Health Services, if applicable.

2. Fundamentals of the HIA for Custodians

This section will familiarize you with the requirements from three areas:

- Health Information Act
- College of Physicians & Surgeons of Alberta
- CMA Code of Ethics

You will understand what a privacy impact assessment is and when you are required to complete one.

3. Requirements from the *Health Information Act*

A health services provider who is considered a custodian of health information if they are designated as such in the Health Information Regulation. In the clinic setting, physicians are considered custodians.

Who else can be a custodian?

Alberta Health, Alberta Health Services (AHS) and community pharmacists are also custodians. As of September 2010, there is a new list of custodians. Regulated members of health professions are now designated as custodians through Health Information Regulation. The current designations include physicians, pharmacists, optometrists, opticians, chiropractors, midwives, podiatrists, dentists, denturists, dental hygienists and nurses. However, application of the act was deferred until March 1, 2011 for dentists and dental hygienists and until September 1, 2011 for nurses.

A custodian must maintain administrative, technical and physical safeguards to maintain the confidentiality and security of health information; this includes health information that is stored or used in a jurisdiction outside of Alberta or that will be disclosed by the custodian to a person in a jurisdiction outside of Alberta.

Each custodian must establish or adopt policies and procedures that will facilitate the implementation of the HIA and the Health Information Regulation.

Custodians have the power to enter into agreements with **information managers** to process, retrieve, or dispose of health information; in accordance with the regulations, strip, encode or otherwise transform, individually identifying health information to create non-identifying health information; and provide information management or information technology services.

After custodians have entered into an agreement with an information manager, the custodian may disclose health information to the information manager without the consent of the individuals who are the subjects of the information for purposes authorized by the agreement.

Resources:

HIA at a Glance for Custodians

Link to the Health Information Regulation

What is a Privacy Impact Assessment and when is One Required?

What is a privacy impact assessment?

A privacy impact assessment (PIA) is a process of reviewing and documenting the types of information that an organization has, reviewing potential risks and determining mitigation strategies.

The PIA is a due diligence exercise in which the organization identifies and addresses potential privacy risks that may occur in the course of its operations. Preparing a PIA entails the review and development of clinic policies and procedures which are the requirements of good office practices and good business.

A PIA assists in reviewing and identifying the impact initiatives or changes in existing processes and systems that collect, use and disclose health information may have on the privacy of patients.

When is a PIA required?

- The HIA requires custodians of health information to prepare PIAs and submit them for review by the Office of the Information and Privacy Commissioner (OIPC) of Alberta before implementing an initiative that affects how health information is collected, used and disclosed.
- A PIA is required when an initiative will affect how individually identifying health information is collected, used and disclosed.
- Examples of initiatives that require a PIA include, but are not limited to:
    - migration of data to a new EMR system
    - using wireless internet connection to connect to an EMR system
    - outsourcing of transcription services

What is included in a PIA?

- Set of written policies and procedures that mandate privacy and security practices and procedures within the clinic
- Information management good practices
- Templates, checklists and other resource documents that can be used immediately within the clinic

Risks of not having safeguards in place to maintain the privacy and security of health information:

- Privacy breach of patient health information that may result in:
    - Negative impacts to physician reputation and professional license
    - Loss of confidence from patients and business partners
    - Errors or disruption to the patient's continuing care and treatment
    - Re-work for physician and office staff

- Patient complaint and subsequent investigation by the OIPC

It is highly recommended that physicians download the document Privacy Impact Assessment Requirements from the OIPC web page on PIA Requirements.

Information Manager Agreements

Custodians must enter into an agreement with an information manager to provide a number of health information management and technology services. Information managers are considered affiliates of a custodian. Health information may be provided to information managers without consent of the individual for the purposes authorized by the agreement.

The HIA defines the term "information manager" to mean a person or body that:

- Processes, stores, retrieves or disposes of health information;
- Strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, in accordance with the regulations; or
- Provides information management or information technology services.

Custodians who require information managers must enter into a written agreement that covers:

- Services to be provided by the information manager;
- All requirements specifically listed in the regulations; and
- That the information manager must comply with the HIA, the regulations and the agreement with the custodian.

Custodians may serve as information managers to other custodians. For example, AHW serves as the information manager to all participating custodians in the Alberta electronic health record.

Custodians who enter into an agreement with an out-of-province information manager must ensure that the agreement contains specific privacy and security safeguards as outlined in the regulations.

Source: Health Information, A Personal Matter: A Practical Guide to the Health Information Act, Office of the Information and Privacy Commissioner of Alberta

4. Requirements from the Health Information Regulation

A custodian must maintain the security of health information. A custodian must designate an individual who is responsible for the overall security and protection of health information in the custody or under the control of the custodian (Privacy Officer). Maintaining the security of health information includes but is not limited to the following activities:

- A custodian must identify, and maintain a written record of its administrative, technical, and physical safeguards in respect of health information.

- A custodian must designate an individual who is responsible for the overall security and protection of health information in the custody or under the control of the custodian (Privacy Officer).
- A custodian must periodically assess its administrative, technical and physical safeguards.
- A custodian must enter into a written agreement that addresses privacy and security requirements with the person/vendor prior to allowing a person/vendor to use or store health information in a jurisdiction outside of Alberta or that is to be disclosed to a person/vendor in a jurisdiction outside of Alberta (this may not apply to health information used to provide continuing treatment and care to a patient).
- A custodian must ensure that its affiliates are aware of and adhere to all of the custodian's administrative, technical and physical safeguards in respect of health information.
- A custodian must establish sanctions that may be imposed against affiliates who breach, or attempt to breach, the custodian's administrative, technical and physical safeguards in respect of health information.

The rules for collection, use and disclosure of health information by custodians also apply to their affiliates, so custodians must ensure affiliates are aware of and follow the same rules.

Who are affiliates?

Affiliates include:

- An individual employed by a custodian
- A person performing a service for a custodian

Custodians are responsible for their affiliates. When affiliates collect, use or disclose information, they do so on behalf of custodians. When patients provide information to affiliates, it is as if they had given the information directly to the custodian. If an affiliate does something the Act forbids them to do, it is as if the custodian performed the act. Affiliates must comply with the Act and regulations as well as with the policies and procedures adopted by their custodians.

Clinic Privacy Officer

You're not in this alone – a clinic Privacy Officer provides critical care for your clinic's patient health information.

A key step in protecting privacy in any clinic is the appointment of a designated Privacy Officer to oversee all the clinic's privacy and security efforts and ensure compliance with HIA within the clinic. This clinic role is a requirement under HIA. Your clinic's Privacy Officer is the "go to" person for information on the HIA, the clinic's privacy and security policies, and privacy practices or emerging issues. The Privacy Officer can be a physician from the clinic or a responsible affiliate who effectively communicates with the custodian. The custodian is ultimately responsible for the collection, use and disclosure of health information.

Each physician office must have a designated Privacy Officer whether you have paper patient records, electronic records or a mix of the two.

- It is vital that everyone in the clinic knows who the Privacy Officer is so incoming requests and emerging issues can be referred appropriately.
- The Privacy Officer usually performs the duties of a security officer since privacy and security are closely related, especially in the context of HIA compliance. However, it is important to note the Privacy Officer will often depend on the electronic medical record (EMR) vendor for many security functions, especially those of a technical nature. This is particularly true of an EMR delivered by an application service provider (ASP), for which the physician office has little direct control over the vendor's computing infrastructure.

5. Requirements from the College of Physicians and Surgeons of Alberta

College of Physicians & Surgeons of Alberta – Health Professions Act Standards of Practice

The College of Physicians & Surgeons of Alberta (CPSA) Health Professions Act Standards of Practice requires physicians to maintain safeguards to protect confidentiality and to protect against reasonably anticipated threats or hazards to the security, integrity, loss or unauthorized use, disclosure, modification or unauthorized access to health information.

CPSA Standards of Practice and FAQs

CPSA Medical Records Policy

How long must I keep patient records and medical recordings (including deceased and minor individuals)?

- A minimum of 10 years, following the date of the last patient visit.
- Minor patients (under 16 years) - at least two years past the age of majority (18 years) or for 10 years, whichever is longer.

How long must I keep X-ray films and reports?

- Films must be kept for at least five years, except for the following cases:
  - Minor patients (under 16 years) - minimum five years, or two years after the patient reaches the age of majority, whichever is longer
- Reports must be kept for at least 10 years
- Mammography films must be kept for a minimum of five years, up to a maximum of 10 years, when there are no intervening studies.

Must a log be maintained of archived and records?

The HIA requires custodians to implement reasonable controls to protect the privacy of health information in their custody or control. A best practice to accomplish this is for custodians to maintain a log of all records archived and destroyed. This also protects the custodian from a medico-legal perspective as there is a record of what has happened to the records.

Other Resources:

The OIPC website (OIPC Questions and Answers) contains a long list of useful questions and answers that cover areas such as:

- patient requests
- legal guardian requests
- insurance company requests
- fees for copies of medical records
- research

Information Sharing Agreement

An Information Sharing Agreement (ISA) is the legal contract that defines the data stewardship rules and processes that the parties have agreed to. It establishes the roles, expectations and accountabilities of each of the parties in their stewardship of the medical information in their custody.

Key elements of an ISA include:

- Identification of the needs and objectives of the key stakeholders
- Principles that guide the development and maintenance of the agreement
- Details of the information uses and disclosures
- Details of the products and services available
- Transition services (entering and exiting the agreement)
- Record retention and access
- Definition of the service levels
- Roles and responsibilities of each party to the agreement
- Financial and legal terms
- Governance and administration processes (including the makeup of the governing body and the dispute resolution process)

The ISA represents the operational application of health policy by physicians, and is a major determinant in the structure and processes in electronic medical record (EMR) deployments and other medical record initiatives.

Source: Data Stewardship Principles, Information Sharing Agreements, Version 1.3
March 2009, College of Physicians and Surgeons of Alberta

For more information, visit the Data Stewardship Information from the College of Physicians & Surgeons of Alberta.

A. Scenario 1 – ID Theft

How real is the risk that someone would want a copy of my patient records? Unless I have someone well known or famous in my clinic, which I don't, I can't imagine why anyone would want my patient's information. As the article states below, I could see Medical ID theft as an issue in the United States, but surely not in Canada.

Smart Card Alliance: Medical ID theft one of fastest growing crimes

There are a number of reasons strong identification is needed in health care. Making sure the correct electronic health record is connected to the correct patient would be the foremost but there's also the growing crime of medical identity theft, according to a report released from the Smart Card Alliance.

"Many authorities consider medical identity theft one of the fastest growing crimes in America," the report states. "With the digital age of health care upon us, the risks are expected to increase as electronic medical records become more prevalent and the exchange of this data over expanding networks becomes more pervasive. Heightened concern over personal data security and privacy highlight the importance of having secure electronic medical identities.

Source: Digital ID News, Wednesday, April 10, 2010

Applying the Principles of the Health Information Act

Identity theft is one of the fastest growing crimes in Canada. Protect your personal information and you will protect yourself against identity theft. Identity theft occurs when personal information (social insurance number, credit card, birth certificate, driver's license or other identifying information) is used without an individual's knowledge or consent to commit a crime, such as fraud or theft.

Whether it is "medical identity theft" or "identity theft", there is a real risk in a clinic that does not have the required safeguards in place. The bottom line is that an Alberta Health Care (AHC) number is a primary source of identification in Alberta. Theft of a patient's AHC number and associated information (such as name and address) puts the patient at a high risk for identity theft. The sale of AHC numbers and personal information is a growing market in Alberta.

Similarly, a physician's practice identification number (Prac ID number) is another source of identification for a physician. Imagine if someone were to falsely set up practice in your name in another country with information they obtained from your office.

In a physician clinic, a custodian is required to maintain the confidentiality and security of health information. If a clinic has its administrative, technical and physical safeguards in place, the risk of ID theft is strongly reduced.

B. Scenario 2 – Passwords

As a physician, I agree with the following quote from the Wall Street Journal. The physician's priority is patient care and many of us work in multiple systems. It's not practical to create strong passwords for all the systems we use and not keep a written record somewhere. Really, is there a practical solution to logging off of terminals and password management?

"For example, the companies that design EMRs assume that the doctors only work within one health-care system. Actually, many doctors work in multiple health-care systems, each of which has its own different brand of EMRs. As each brand of EMR demands that the doctors regularly change their passwords, and as each password change occurs on a different random date, most doctors use such trivial passwords that any respectable hacker should be able to access the passwords in less than five minutes. Also, as you wander around any hospital, you are certain to find a computer terminal that someone has forgotten to log off from, leaving medical information open for all to see."

Source: The Wall Street Journal, March 30, 2010, Letters "Industry Rep Calls Patient Privacy 'Overblown' Worry"

Password Management

Password management doesn't have to be complex if you develop your own unique system and do not share it with anyone. If all staff and physicians adhere to best practices, risk is substantially reduced.

- Staff must not place passwords on sticky notes or in drawers - this is not acceptable in clinic environments
- Password tips:
  - Keep them long (minimum eight characters).
  - Use a space as a character if your system allows it, otherwise use the symbols on the keyboard. Use uppercase and lowercase letters as well as a number.
  - Don't share passwords across accounts (i.e., business and personal or between hospital and clinic).
  - A help desk never asks for your password.
  - Regular password changes are necessary.
- Create your own unique system for password management. Develop this system, don't write it down and don't share it with anyone. The resulting passwords should be something that you can remember and easily generate the next password when prompted by your system. Take time to develop your own personal system so it means something to you and ensure it is confidential.

Alberta Netcare Password Guidelines

Purpose: Ensure that privacy and security of our computer systems are maintained by using a strong password standard.

Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff except for security purposes. Unique passwords or other authentication controls are required for each desktop, network, server, EMR, etc.

All monitors used to display Alberta Netcare or other identifying health information will time out after a short period of inactivity and require a password to reactivate the screen. Selected time-out periods must reflect the level of risk of exposure of workstations. Each new employee is given clear directions on how to create a new password for network access and each application.

The following are minimum complexity rules requirements for password development:

- A minimum length of eight characters
- No embedded part of name
- Use three of the following – alpha-upper case, alpha-lower case, numeric, special characters
- Maximum validity days of 90
- 24 iterations required before reuse
- Five maximum invalid attempts before account lockout

The password must contain characters from at least three of the following four categories:

Group	Example
Lowercase letters	a, b, c ...
Uppercase letters	A, B, C ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	()'~!@#$%^&*-+=|\{}[]:;"'<

Reference: Alberta Health: http://www.albertanetcare.ca/LearningCentre/Access-Passwords.htm

How Not to Choose a Password

Here are some of the types of passwords that will be picked up by password crackers:

- Any name (crackers don't necessarily know that your aunt's middle name is Agnes, but it's easy enough to get a list of 100,000 names and try each one).
- Any word in any "cracking dictionary." There are lists of words that crackers use to try to crack passwords, and these are passwords that a lot of people use. Some of these lists include: abbreviations, asteroids, biology, cartoons, character patterns, machine names,

famous names, female names, bible male names, movies, myths and legends, number patterns, short phrases, places, science fiction, shakespeare, songs, sports and surnames.

- Any of the above, with a single character before or after it ("8dinner", "happy1").
- Any of the above, capitalized ("cat" -->"Cat")
- Any of the above, reversed ("cat" -->"tac"), doubled ("cat" --> "catcat") or mirrored ("cat" --> "cattac").
- We used to tell people that taking a word and substituting some characters (a 0 (zero) for an o, or a 1 for an l) made a good password. This is no longer the case. New crackers have the capability to crack things like this, in certain situations.
- Words like "foobar", "xyzzy" and "qwerty" are still just plain words. They are also popular passwords, and the crack programs look for them. Avoid them.
- Any of the sample passwords, good or bad, mentioned in this document.

Source: http://www.cs.umd.edu/faq/Passwords.shtml

How to Choose a Good Password

Coming up with a good password can be difficult, these guidelines can help you to develop a strong password.

- Choose a password that is at least eight characters long. This should be long enough to discourage a brute-force attack. Currently, the maximum password length on many Unix systems is eight characters, but if you want to add a few more characters to make it easier to remember, go ahead. Just bear in mind that anything after the eighth character will be ignored (so "abnormalbrain" is the same as "abnormal").
- Strong passwords have a mix of lower and upper-case characters, numbers, and punctuation marks, and should be at least eight characters long. Unfortunately, passwords like this are often hard to remember and result in people writing them down. Do not write your passwords down!
- ***The license plate rule:*** take a phrase and try to squeeze it into eight characters, as if you wanted to put it on a vanity license plate.
- Some people like to pick several small words, separated by punctuation marks.
- Put a punctuation mark in the middle of a word, e.g., "vege%tarian".
- Use some unusual way of contracting a word. You don't have to use an apostrophe.
- One of my favorite passwords was "kEp*-h&y": "kEp" -->"keep", "*-" --> "laser" (like those signs that you see outside of physics labs), and "h&y" --> "handy"; "Keep your laser handy!"
- You can use control characters. Just bear in mind that a lot of them have special meanings. If you use ^D, ^H or ^U, for example, you might not be able to log in again.
- Think of an uncommon phrase, and take the first, second or last letter of each word. "You can't always get what you want" would yield "ycagwyw". Throw in a capital letter and a punctuation mark or a number or two, and you can end up with "yCag5wyw".

- Deliberately misspelling one or more words can make your password harder to crack.
- Use several of the techniques above.
- Something that no one but you would ever think of. The best password is one that is totally random to anyone else except you. It is difficult to tell you how to come up with these, but people are able to do it. Use your imagination!

Reminder: Do not use any of the sample passwords above.
Source: http://www.cs.umd.edu/faq/Passwords.shtml

Risk of Wireless Internet

Wireless systems that are set up without adequate security put a clinic at risk of a sophisticated hacker.

Recommended practices include unplugging the access point(s) after office hours and running a daily scan of the wireless network to ensure there are no rogue and/or unauthorized connections.

On an annual basis review and update the inventory of wireless devices and other hardware peripherals connected to the clinic's network.

C. Scenario 3 – Need to Know

I'm a physician and my clinic is using an EMR. The children of several staff members are patients in the clinic. This has led to two concerning situations.

Situation 1: One of the staff that works at my clinic presented a signed note from her adult child stating that she may have access to her adult child's health record on an ongoing basis. The adult child is not a legal dependent of the staff member who is the receptionist. The adult child has diabetes and requires frequent care at the clinic. Can the receptionist have regular access to her adult son's record?

Situation 2: I am providing care for one of my patient's spouses who requires a referral to a specialist. The clinic's referral clerk is my patient's wife. Can the wife process the referral as part of her regular duties as the referral clerk? Do I need to disrupt my regular workflow to have this referral completed by another staff member?

Applying the Principles of the Health Information Act (HIA)

Both these situations have one thing in common: an affiliate's access to health information.

Clinic staff are the affiliates of a custodian in a clinic setting. Affiliates must only collect, use and disclose health information in accordance with their duties to the custodian. In general, follow the "need to know" principle. An affiliate is required to have access to the health information that is required as part of their regular duties to support care of the patient in their role. Affiliates sign an oath of confidentiality that requires him or her to follow the clinic policies and procedures and to not disclose information.

Situation 1: The receptionist, as part of her regular duties, would not require access to the full patient record of her son (or any other patient). On the "need to know" principle no clinic staff member would have "at will" access to any patient record that they produced a consent note for, including their own or a family member's. Staff must understand that the clinic's EMR can be audited if a complaint is filed to determine who has accessed a patient's health record.

Situation 2: It is irrelevant who the patient is. The referral clerk requires access to specific information on a regular basis that is required to process referrals for physicians. The referral clerk has signed an oath of confidentiality and cannot disclose to her husband, or any other patient, information that is acquired as a requirement of her regular duties.

Staff should have a good understanding of the privacy and security policies and procedures in a clinic setting. Clinic policies and procedures need to be reviewed and discussed regularly. Especially in rural settings where there are a limited number of care providers and staff for the patient population, the "need to know" principle always applies: "Collect, use, and disclose health information only as necessary to achieve an intended purpose. Employees or others involved in direct patient care should only have access to information about patients for whom they are responsible or are providing care to". Once a physician or staff member acquires health information they are required to keep it confidential.

Clinic self-audits:

A best practice is for a clinic manager to produce, on a regular basis, an analysis of the clinic's audit reports. A common EMR report that is regularly performed at clinics is a "same name search" of staff members. Refer back to your clinic's PIA, it will provide the listing of all role based access.

Resources

What are the components for an affiliate's oath of confidentiality?

A statement, sworn (or affirmed) by the affiliate, stating that:

1. He/she will uphold to the best of his/her ability his/her duties under the Health Information Act and the regulations and the custodian's policies and procedures, and that
2. He/she will not disclose or make known any recorded or non-recorded health information of an individual except as authorized by the act, the regulations and the custodian's policies and procedures.

Space for the city, town, village, etc. where the oath is sworn.

Space for the date and signature of a witness.

Adapted from Health Information Act: Guidelines and Practices from Alberta Health

D. Scenario 4 – Visual Privacy

Our clinic practice has been located in the same building for the last 15 years. Three years ago we decided to install an EMR. The clinic front office and exam rooms were never designed to have computer monitors in them. As a result, our physical site does not offer good screen viewing protection. Keeping our office workflow moving is our priority. How do you practically balance office layout for ease of use vs. screen viewing protection?

Applying the Principles of the Health Information Act

Balancing ease of use and screen viewing protection can be a challenge for offices that have transitioned from being paper-based and are not in a facility designed for workstations to exist throughout the clinic.

Simple Solutions

- Use of privacy screens or filters. Monitors that have a built in privacy screen or an added filter ensures that only the person sitting directly in front of the monitor can see the images on screen. Passersby see only a dark screen or blurred image. This limits the field of view of the monitor and can help clinics ensure privacy. Filters can be an economical add-on to your existing monitors.
- Turning or tilting the monitor can also be a simple solution.
- Clinic layout can be adjusted to ensure patient privacy is protected. Spend some time with your staff considering potential changes to your clinic layout and workflow. Consulting a privacy specialist can be valuable when you need extra help.
- Ensuring clinic staff adheres to policies and procedures regarding logging into and out of computer stations provides protection that workstations are not left unattended with easy access to patient files.

Unauthorized viewing of computer screens and unattended live screens puts a clinic and its health information at risk. Clinic staff should be reminded to apply best practices to maintain the privacy and security of your clinic's health records.

Speech Privacy

While visual privacy is a common issue, overhearing private conversations and patient examinations is a problem in some clinic sites. While background music in waiting areas is of assistance, some clinics should explore the technology of sound masking.

Sound masking means to add natural or artificial sound (commonly, though inaccurately, referred to as "white noise") into an environment to cover unwanted sound by using auditory masking. This noise reduction technique is accomplished by playing a consistent, harmonious background sound to mask private conversations.

Sound masking reduces or eliminates awareness of pre-existing sounds in a given area and can make a work environment more comfortable, while creating speech privacy so workers can better concentrate and be more productive. This technology may be of assistance in clinics where conversations are overheard at the reception area or sound passes from one exam room to another.

E. Scenario 5 – User Controls

I'm a physician in a small office of three doctors and a trusted group of staff that have worked together for a long time. When we first installed our EMR, we had our privacy and security settings set to the maximum and found it interrupted our workflow. We changed the settings to allow all staff to have complete access to the patient records. Everything has worked fine for years until recently we hired a temporary staff member when one of our long-time staff required a leave of absence. We think the temporary staff member may be looking at the health records of other staff who are patients at the clinic. We haven't looked at our EMR's privacy settings in years, how do we manage our privacy and security settings in our EMR? How can we tell if the temporary staff member is looking at the records?

Applying the Principles of the Health Information Act

In this scenario, understanding technical and administrative safeguards is key.

Administrative Safeguards

It is important to be aware that all clinic staff including contractors, interns, volunteers, cleaning staff and temporary employees must sign an oath of confidentiality prior to starting their clinic duties. Consequences for a breach in confidentiality or unauthorized viewing of health records must be made clear to all clinic staff and be outlined in your clinic's policies and procedures.

Clinic affiliates need to understand that access to patient records is continually on a "need to know basis" and that your EMR monitors access to patient records. Remind clinic staff that sharing user IDs within the EMR and Netcare is strictly prohibited.

Limiting disclosure by a custodian's affiliates (including employees and contractors)

Clinics require a policy requiring staff, students and contractors with access to health information in paper or electronic format to sign an Oath of Confidentiality.

The following are the general rules for affiliates who are employees, contractors, students, residents and volunteers in a physician office:

- Must safeguard the health information they hold
- Only disclose what is needed to do the job, no more
- Provide anonymous information wherever possible
- Only provide information to those who need to know

Adapted from *The Health Information at a Glance for Custodians* by the OIPC

What is a vendor non-disclosure agreement (VNDA)

A vendor non-disclosure agreement (VNDA) is used if a clinic has a vendor that may have short-term or potential access to health information maintained by a custodian. The agreement assumes that some, all or part of the information viewable by the vendor is health information.

Examples include on-site repair of computer equipment, on-site wireless networking, cleaning service, annual destruction of inactive files by third party shredding company.

Technical Safeguards

Security settings:

Your EMR has security settings that help to protect your clinic. EMR systems that conformed to VCUR 08 or VCUR 06 have the ability to assign user based access, role based access and context based access to the EMR. When you assign user based access to the EMR, it ensures that only physician and office staff have access to patient information.

When you assign role based access controls, users are grouped by functional area in the EMR which creates the ability to group users and apply specific security rules per group. When context-based access rights are assigned or restricted based on the context of the transaction (e.g., location, time, functional area) control over data access in both temporal and geographic terms is improved.

Audit controls and reports:

You can run an audit report to determine what patient information your staff has been viewing in the EMR. The information your staff have been viewing should follow the "need to know" principle. Inform your staff that this will be a regular occurrence at your clinic and ensure they are aware of the consequences of viewing information outside their role and responsibilities.

Turning off the audit log is a breach of a clinic's PIA but this is possible in some older EMR systems. Audit logs are mandatory under the HIA. In the case of a privacy breach, the OIPC will request the audit log.

Not sure how to set the security settings and run the reports in your EMR? Contact your vendor for support as each system has unique settings.

F. Scenario 6 – Reusing Paper

Our office staff are vigilant about the amount of paper that we use and feel that, as good environmental stewards, we should conserve paper in the clinic. After this topic was brought up at a recent staff meeting I noticed that one clinic staff member was using the clean side of clinical documents (incoming faxes) as printer paper and scrap paper to conserve paper. Another staff member mentioned that the cover page is a waste of paper on outgoing faxes and proposed we eliminate that page from our outgoing faxes. Is there a compromise between environmental stewardship and privacy and security?

Applying the principals of the Health Information Act

There are two important issues that need to be addressed with this scenario:

1. **Management of printed documents in the clinic that are second copies and do not need to be stored.**

Secure shredding is essential. Duplicates should be destroyed in such a manner that the information is illegible. Clinics should use a confidential shredding or destruction service.

- Privacy and security breaches are often not malicious acts but due to lack of information, policies and training. In this scenario staff have noble intentions in mind, being stewards of the environment. Unfortunately, the staff members need to understand the importance and clinic administrative policies regarding retention and storage of documents.
- Investigate technology to receive your incoming faxes electronically, they need not be printed and can be attached to a patient record in the EMR. Speak to your vendor about electronic fax management: sending and receiving your faxes electronically and eliminating paper. Remember that your PIA will need adjustment when you add new hardware in your clinic.

2. Importance of a fax cover sheet.

Without the fax cover sheet, you cannot track the information. The confidentiality clause on a fax cover sheet is required and eliminating that text on a fax puts the physician at risk.

Resources:

If you have not done so yet in this tutorial, it is recommended to visit the questions and answers on the HIA at the OIPC web site: OIPC Questions and Answers

G. Conclusion

Maintaining the privacy and confidentiality of the health information in your clinic means applying administrative, physical and technical safeguards. Review your clinic's polices on a regular basis and discuss with your clinic privacy officer and staff.