General Privacy Training

Published: February 2015

Alberta Netcare ELECTRONIC HEALTH RECORD

Contents

The information in this training is provided for education and guidance only and is not intended to replace expert advice.

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

Introduction

Welcome to General Privacy Training. This training will take you approximately 60 – 90 minutes to complete. You can finish this training in several sessions and resume where you left off each time you return.

The purpose of this training is to provide a resource for clinicians and staff to ensure their privacy and training knowledge is in line with the Alberta *Health Information Act* (HIA).

Learning Objectives

- To identify the principles of the HIA
- To apply the HIA in practical scenarios in a clinic setting with electronic medical records (EMRs)

Module 1: Introduction

What is health information and how does the HIA protect the health information of Albertans?

This module will help all clinic team members to become aware of basic rules and principles within Alberta's HIA.

Clinic PIA Tip
Throughout the General Privacy Training program, you will find tips that relate to your clinic's privacy impact assessment (PIA) preparation. This will help you understand what is required in the preparation of your PIA and includes what information is available in your PIA.

The Health Information Act

The HIA contains rules about the collection, use, disclosure, access to and protection of health information.

Collection
Collection is defined as the means to gather, acquire, receive or obtain health information as per Section 1(1)(d) of the HIA.

Examples of collection activities include but are not limited to:

- Taking a medical history
- Having individuals complete forms to provide health information
- Having individuals respond through surveys, questionnaires or polls for research purposes

Clinic PIA Tip
Your clinic's PIA provides an overview of privacy information that is pertinent to the operation of your clinic's electronic medical record (EMR) solution and the patient health records that it manages. A PIA contains six sections that address different aspects of privacy and security for your clinic.

Part 3 (Sections 18 to 24) and Part 6 (Sections 57 and 58) of the HIA contain rules governing the collection of health information.

Use
Use is defined as applying health information for a purpose, and includes reproducing information. It does not include disclosing information.

Part 4 (Sections 25 to 30) of the HIA contains rules governing the use of health information.

Disclosure
Disclosure refers to providing health information to someone other than the individual the health information is about, usually to a third party. It can be defined as the release, transmittal, exposure, revealing, showing, providing copies of, telling the contents of or giving health information by any means to any person or organization; it includes disclosure to another custodian or non-custodian.

Part 5 (Sections 31 to 56) and Part 6 (Sections 57 and 58) of the HIA contain rules governing the disclosure of health information. Sharing health information in a clinic's EMR solution or Alberta Netcare is considered a "use", not a disclosure.

Access
Access includes providing an individual with access to their health information both informally or in response to a formal access request.

Under Section 7(1) of the HIA, an individual has the right to access any record containing health information about that individual that is in the custody of or under the control of a custodian (subject to limited exception per the HIA).

Protection
The protection of health information involves the use of administrative, technical and physical safeguards. These safeguards will be discussed in later modules of this training session.

Section 60 of the HIA and Section 8 of the HIA's Health Information Regulation requires custodians (including physicians and regulated health professionals) to protect health information. These rules apply to health information in any form (such as recorded or non-recorded), format or information system.

Responsibilities under the Health Information Act

As of April 2001, health information in Alberta became protected under the HIA. The HIA requires that:

- Individually identifying health information is disclosed with the individual's consent or statutory authority unless otherwise permitted under the HIA
- Research ethics board approval is obtained for use or disclosure of health information for research (HIA Section 49 and 50)
- The Office of the Information and Privacy Commissioner be notified of any data matching initiative that involves non-custodians (HIA Section 32(2))
- PIAs must be completed and submitted to the Commissioner (HIA Section 64(1)(2))
- Custodians take reasonable steps to provide administrative, technical and physical safeguards of health information including written policies and procedures (HIA Section 60 and Health Information Regulation 8)
- Custodians take appropriate measures to protect the security and confidentiality of electronic health records (HIA Section 60(2)(a))
- Custodians enter into written agreements before disclosing information to researchers, information managers or to recipients outside of Alberta (HIA Section 66)
- Custodians disclose only aggregate information whenever possible (HIA Section 57)
- Custodians disclose only the least amount of information for the intended purpose (HIA Section 58(1))
- Custodians consider the expressed wishes of the individual before disclosing information (HIA Section 58(2))
- Custodians keep a notation of all disclosures and provide individuals with access to that information upon request (HIA Section 41)

Disclosure outside these rules contravenes privacy legislation. Remedies are available and can be initiated with a complaint to the Office of the Information and Privacy Commissioner.

Health Information

What Information Qualifies as Health Information?
The HIA defines health information as meaning any or all of the following:

- Diagnostic, treatment and care information
- Registration information

Clinic PIA Tip
Project Privacy Analysis in Section C of your PIA summarizes the health information your clinic's EMR may include. Review this carefully to understand how health information is handled in your EMR.

Diagnostic, Treatment and Care Information
Diagnostic, treatment and care information is any information about an individual's health and health services provided to that individual including the cost of such services. This type of information is what health care professionals deal with on a regular basis.
Examples:

- A person's physical or mental health status
- Medical procedures and treatments applied to an individual
- Prescriptions issued
- Medical advice provided
- Medical history
- Blood test results
- Medical devices and/or aids issued to an individual
- Health services provider information

Section 1(1)(i) of the HIA contains the definition of diagnostic, treatment and care information.

Registration Information
Registration information is any information about an individual that falls into one or more of the following categories:

- Demographic information
- Location
- Telecommunication information
- Residency information
- Health services eligibility information
- Billing information

Examples:

- Name
- Age
- Gender
- Home address
- Phone number
- Citizenship
- Personal health number

- Billing account number
- Amounts owed

Section 1(1)(u) of the HIA contains the definition of registration information.

Collecting Health Information

Collecting Health Information from Patients

When it comes to individually identifying health information collected directly from patients, the HIA states that physicians must take reasonable steps to inform the person of:

- The purpose for which information is being collected
- The specific legal authority for collecting the information

Physicians will need to exercise their good judgment and common sense as it is not practical or necessary to have a conversation about collection with every patient. Brochures, notices or signs help to comply with this portion of the act.

Purpose and Legal Authority for Collecting Information

Under the legal authority of the HIA, individually identifying personal health information can be used for:

- Providing a health service
- Determining or verifying eligibility to receive a health service

Other authorized purposes for collection of individually identifying health information include conducting investigations, holding discipline proceedings, educating health service providers and conducting research.

Individually identifying health information may also be collected if the collection is authorized by an enactment of Alberta or Canada, for example the reporting of a communicable disease under the Public Health Act.

Ensuring Accuracy and Completeness

Custodians must make reasonable effort to ensure that information is accurate and complete before they use it. In most instances, reasonable effort would include assessing if the information is:

- Current
- Accurate
- Complete
- Relevant
- Not misleading

Reasonableness may depend upon the circumstances. Apply caution if the information was collected by a third party or if the patient provides the information directly but seems confused or unsure.

Best Practice
There should be careful verification of any health information crucial to an application, transaction or action when the information is provided. There could also be systematic processes in place for updating health information, either as a result of information provided from the individual or cross-referencing other related files providing basic identifying data.

Patient Questions about the Collection of Health Information
Patient questions may often be asked in the examining room when physicians may or may not have time to deal with them. When this discussion cannot be carried out, the HIA requires that a physician's office have a designated individual—physician or staff member—who will be the key contact for HIA matters.

Custodians and Affiliates

To whom does the HIA apply?

Custodians
Custodians include:

- Physicians, registered nurses and regulated health professionals
- Pharmacies and pharmacists
- Minister and Department
- Alberta Health Services
- Hospital, nursing home or ambulance operator

For a full definition of custodians, see Section 1(1)(f) of the HIA and Section 2 of the Health Information Regulation.

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

Affiliates include:

- An individual employed by a custodian
- A person performing a service for a custodian
- A health services provider who is exercising the right to admit and treat patients at a hospital

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 HIA forbids them to do, it is as if the custodian performed the act. Affiliates must comply with the HIA and regulations as well as with the health information policies and procedures adopted by their custodians.

Module 1 Quiz

1. In Alberta's HIA, all clinic staff are "custodians" of patient health records and are subject to specific rules dealing with health information.	
☐	**a.** True
☐	**b.** False
2. Alberta's HIA is about the collection, use and disclosure of health information.	
☐	**a.** True
☐	**b.** False
3. Health information only applies to patient care information.	
☐	**a.** True
☐	**b.** False

Module 1 Quiz – Answer Key

1. In Alberta's HIA, all clinic staff are "custodians" of patient health records and are subject to specific rules dealing with health information.

The answer is b. False
The physician is usually the only custodian in the clinic; clinic staff are considered affiliates. Custodians are responsible for their affiliates. When affiliates collect, use or disclose information, they do so on behalf of the custodian. Therefore, affiliates must also comply with the HIA, and it is the custodian's responsibility to ensure their affiliates are aware of and follow the same rules. Each affiliate (clinic staff member) needs to sign an oath of confidentiality.

2. Alberta's HIA is about the collection, use and disclosure of health information.

The answer is a. True
Key points regarding health information in clinics:

- The custodian (usually the physician) is the gatekeeper
- Consent is required
- Disclose the least amount of information necessary
- Use the highest degree of anonymity
- Disclose information on a need-to-know basis

3. Health information only applies to patient care information.

The answer is b. False
Health information is more than patient care information and means any of the following:

- Diagnostic, treatment and care information
- Health services provider information
- Registration information

Module 1 Summary

Health information includes:

- Diagnostic, treatment and care information
- Registration information

Administrative safeguards and your clinic's health information policies and procedures safeguard and uphold the collection, use, disclosure, access and protection of health information.

Module 2: Privacy, Security and Confidentiality

Privacy, security and confidentiality are fundamental requirements of Alberta's *Health Information Act* (HIA). Custodians and affiliates must follow these requirements to protect the personal health information of their patients and clients.

This module will help you understand the HIA requirements regarding privacy, security and the confidentiality of health information.

What is Privacy?

Privacy can be defined as:

- The right of an individual to be able to control access to their personal information as well as the collection, use and disclosure of his or her information
- How health information is protected from external sources and how it is monitored to control access to as well as the collection, use and disclosure of patient health information

HIA Privacy Principles

The following HIA privacy principles are the guideposts that structure how your clinic will collect, use or disclose health information.

Principle 1 – Accountability and Management
Clinics are accountable for the health information that patients give them.

Principle 2 – Notice
Clinics explain why they collect individually identifying health information before it is collected.

Principle 3 – Collection
Clinics limit the amount and type of health information they collect.

Clinic PIA Tip:
Your clinic's privacy impact assessment (PIA) includes a Privacy Charter in the Health Information and Security Manual. This charter contains 10 privacy principles that form the basis of the HIA and will help guide how your clinic collects, uses and discloses health information.

Clinics adopt this privacy charter as part of their PIA and apply these principles to ensure protection from privacy breaches.

Principle 4 – Use and Disclosure
Clinics use and disclose patient health information only for the reasons for which it was provided, unless otherwise permitted by law.

Principle 5 – Consent
Clinics may disclose patient health information to a third party with the patient's written consent to that disclosure.

Principle 6 – Access
Patients have a right to access their health information that is in a clinic's custody or control with the provisions of the HIA.

Principle 7 – Safeguards
Clinics protect patient health information from unauthorized access, use, disclosure or destruction.

Principle 8 – Quality
Clinics take effort to ensure patient health information in their custody or control is accurate and complete before using or disclosing that health information.

Principle 9 – Retention and Destruction of Records
Clinics retain patient health information per the College of Physicians & Surgeons of Alberta guidelines and will securely destroy patient health information when it is no longer needed.

Principle 10 – Monitoring and Enforcement
Clinics monitor compliance with privacy policies and procedures, and have a process for complaints about the handling of health information in the clinic.

Privacy Breaches

A privacy breach can take place in a clinic when there is unauthorized access to, collection of, use of, disclosure of or disposal of personal or health information.

Willful and deliberate misuse or abuse of health information may be the result of idle curiosity, but such actions may also be taken with malicious intent. This is grounds for prosecution under the HIA, as misuse of health information is a serious violation of the act.

Clinic PIA Tip
Your clinic's PIA includes a section on Privacy Breach Management in Section B, Organizational Privacy Management.

Be sure to review this section carefully so you are knowledgeable about and aware of your responsibilities should a privacy breach occur in your clinic.

Prosecution Under the HIA
It is an offense under the HIA to knowingly obtain or attempt to obtain access to health information in contravention of the HIA. Commission of such offenses is punishable by fines of up to $500,000.

Professional Penalties
Regulated healthcare professionals in Alberta are bound by the statutes, regulations and standards of their professional regulatory body. They are also bound by the Alberta Health Professions Act.

Professional regulatory bodies conduct investigations into complaints made about members, and the penalties imposed must meet the objective of public protection. Such penalties can include the suspension of practice permits in addition to significant financial fines.

Audits
Alberta Health monitors use and access to the provincial electronic health record system and conducts investigations in cases of suspected abuse or fraud.

Patients are protected and every user access in Alberta Netcare is tracked. Routine audits are conducted on a monthly basis. Additional audits and Office of Information and Privacy Commissioner (OIPC) investigations can be triggered by patient complaints or requests for health information audit logs.

Audit logs are a mandatory component of the POSP electronic medical record (EMR) solutions. It is recommended that audit logs be reviewed quarterly by the clinic's privacy officer to ensure clinic employees are acting responsibly with access to patient health information.

Errors that Result in Privacy Breaches

The following information outlines the most common privacy errors that result in privacy breaches, and provides you with an outline of steps to diminish the chance of these errors happening in your clinic.

1. Inappropriate access to health information
Clinic employees with access to the personal healthcare records of patients need to be aware of the risks involved with unauthorized or inappropriate access of personal health records.

Adapt and apply the following privacy guidelines in your clinic:

- No one can collect, use, access or disclose health information other than to achieve an intended authorized purpose regarding patient care at the clinic. As an employee of the clinic, health information systems may only be used for job-related purposes and not for any other reasons. This also applies to use of external health information systems such as Alberta Netcare.
- Health information should be kept in confidence and not disclosed over the phone without proper identification.
- Adequate training is the key to good privacy practices. Clinic employees need to be aware of and review clinic administrative and technical policies and procedures on a regularly scheduled basis.

2. Misdirected laboratory and diagnostic imaging test results
Alberta's healthcare system requires the successful transfer of patient health information between healthcare providers. This is facilitated through the use of technologies including fax machines and computer systems. Unfortunately, laboratory and diagnostic imaging test results are sometimes sent to the wrong physician or clinic in error.
When this occurs, the following steps must be taken to ensure test results are redirected to the correct physician and clinic.

If you receive an unknown patient's test results in error, it is recommended you respond with the following actions:

- Notify the sender that the results were sent to the wrong physician/clinic.
- Contact the physician who was to receive the test results, and determine if they have or have not received the misdirected test results.
- If the physician has not received the misdirected test results, offer to forward the information to them.
- If the physician has already received the test results, confirm this and ensure that the misdirected test results are destroyed.
- According to the HIA, collecting or keeping health information that you have no authority to collect or use violates the HIA collection principle.

3. Use of clinic fax machines
Health information is transmitted in Alberta via fax on a regular basis, and custodians and healthcare organizations need to be aware of the potential security risks inherent to the use of faxes to distribute health information.

As a custodian, it is your responsibility to ensure appropriate measures are in place to protect patient health information.

Implement the following safeguards in your clinic to reduce the risk of accidentally disclosing personal information when using a fax machine:

- Limit faxing of health information to situations where the information must be faxed and send the most limited amount of information.
- Place fax machines in a secure area away from public view and access.

- Use validated pre-programmed fax numbers where possible (send a test fax to each pre-programmed number to verify accuracy before entering that number in the address book).
- Before sending a manual fax, check that the receiver's number is correct then verify in the fax machine's window that you have keyed it in correctly.
- Always complete a clinic fax cover sheet, clearly identifying both sender and intended receiver of the information. The cover sheet must include a confidentiality notice warning that the information is intended for the named recipient only, as well as a request that a receiver contact you immediately if the transmission is misdirected.
- If you are sending information via a fax modem (fax device contained in a computer), confirm that other users of the computer system cannot access the fax without a password.
- If possible, use encryption technology or other technology to secure fax transmissions.

Security

What is Security?

Security is the means to keep health information private and to maintain accessibility to the integrity of the information. This involves the use of physical, technical and administrative controls or procedures.

Clinic PIA Tip

To help you manage the security risks at your clinic, your PIA contains a Risk Assessment Table that identifies clinic security threats and provides mitigation measures to reduce these threats.

Review the Risk Assessment Table carefully so you can reduce security threats in your clinic.

Physical security involves:

- Applying physical barriers and control procedures against threats (e.g., motion detection alarms and a locked door to the server room or a metal cage around the server)

Technical security involves:

- Using unique user identification and strong passwords
- Using role-based access to limit access to health information to a need-to-know basis
- Using a commercial grade firewall and anti-virus software that is updated automatically
- Monitoring logs of access to health information

Administrative security involves:

- Implementing and updating security policies and procedures in the clinic
- Training clinic staff regularly on security policies and procedures
- Using Information Manager and Non-Disclosure Agreements with contractors, staff and others working in the clinic

Confidentiality

What is Confidentiality?

Confidentiality is the ability to limit the disclosure of health information and ensure only those who are authorized can use or access it. It establishes a trust relationship between the person supplying the information and the individual or organization collecting it.

Section 60 of the HIA mandates that custodians have an obligation to protect health information from unauthorized disclosure. Custodians must make sure that information is not inappropriately used or disclosed to those who do not need to know it.

Avoid discussing patient information in areas where people who do not need to know such information are present. It is important to be aware that those who may overhear may know the identity of the patient being discussed.

Clinic PIA Tip

To ensure clinic employees are aware of and understand clinic confidentiality requirements, maintain an Employee Confidentiality and Security Checklist and EMR Access Request form for each clinic employee.

Both forms are included in Appendix 2, Forms, in the Health Information Privacy and Security Manual in your clinic's PIA. Ensure these forms are completed for each clinic employee.

Inappropriate places to discuss patient health information include but are not limited to:

- Cafeterias
- Public areas such as washrooms and hallways
- Elevators

Real Case Study

A patient was in an exam room with a physician. When the physician left the exam room for a period of time, the patient was alone with a computer containing electronic medical records open for access. A patient record was open on the screen and in clear view. The patient reported the case to the Office of the Information and Privacy Commissioner (OIPC) of Alberta.

Consider:

- Was there a privacy breach?
- What could have been done to prevent this from happening?

Did a Privacy Breach Occur?

Yes, a privacy breach occurred when the physician left the screen open with the patient alone in the room. In this case, with the screen accessible, the computer unlocked and the physician logged in, the patient could have obtained access to the record in front of him and other records in the system.

What Could Have Been Done to Prevent this from Happening?

Administrative and technical safeguards could have been applied. For example, the physician could have logged off or locked the computer before leaving the room (Use the keyboard shortcut ctl + alt + del to lock a computer or go to the Start Menu then Windows Security).

Module 2 Quiz

1. Deliberate misuse or abuse of health information is grounds for prosecution under the HIA	
☐	**a.** True
☐	**b.** False
2. As long as you immediately destroy lab results sent to you in error, you have fulfilled your duty as a custodian.	
☐	**a.** True
☐	**b.** False
3. Using only pre-programmed, verified fax numbers on a fax machine helps to prevent unauthorized disclosure of information.	
☐	**a.** True
☐	**b.** False

Module 2 Quiz – Answer Key

1. Deliberate misuse or abuse of health information is grounds for prosecution under the HIA.
The answer is a. True The privacy of healthcare records is protected under the HIA. Section 107 outlines the restrictions in place for custodians and affiliates access to healthcare information, and outlines the fines applicable for those custodians and affiliates who contravene this section.
2. As long as you immediately destroy lab results sent to you in error, you have fulfilled your duty as a custodian.
The answer is b. False Key points regarding misdirected lab results: • You must notify the sender the results were sent to the wrong physician/clinic • You must contact the physician who should have received the test results, and determine if the test results have or have not been received • If the physician has already received the test results, confirm this and ensure the misdirected test results you received are destroyed
3. Using only pre-programmed, verified fax numbers on a fax machine helps to prevent unauthorized disclosure of information. Using only pre-programmed, verified fax numbers on a fax machine helps to prevent unauthorized disclosure of information.
The answer is a. True Automation can help reduce human error and ensure that faxes go only to their intended destination. Even though a fax machine contains pre-programmed fax numbers, it is still leading practice to call the recipient to confirm they have received the fax.

Module 2 Summary

Privacy, security and confidentiality includes:

- The rules and privacy principles in Alberta's HIA and the professional obligations custodians and affiliates must fulfill under the HIA.
- A clinic's obligation to keep health information private and to maintain accessibility to the integrity of the information. This includes physical, technical and administrative controls and procedures.
- A clinic's responsibility to limit the disclosure of health information and ensure only those who are authorized can use or access it.

All clinic team members, both custodians and affiliates, have a responsibility to understand the rules and privacy principles in Alberta's HIA.

Module 3: Administrative and Physical Safeguards

Why are your clinic's policies and procedures regarding privacy and security vital to how you and the clinic staff handle health information?

This module will help all clinic team members become aware of the importance of:

- Understanding and following your clinic's administrative policies and procedures surrounding privacy and security
- Maintaining physical safeguards that help protect health information

Clinic PIA Tip

Policy 5, Information Handling, of the Health Information and Security Manual in your PIA outlines administrative, technical and physical safeguards for information handling that should be implemented in your clinic.

Review Policy 5 carefully and apply these safeguards to protect your clinic from health information privacy breaches.

Administrative Safeguards

Administrative safeguards are policies and procedures within the clinic that address the requirements for safeguarding health information.

The *Health Information Act* (HIA) requires that reasonable steps be taken to maintain administrative safeguards, and that maintenance goes beyond simply having safeguards in place.

To maintain administrative safeguards, a custodian must take reasonable steps to:

- Implement appropriate policies and procedures
- Educate and train affiliates on the policies and procedures
- Ensure affiliates comply with the policies and procedures
- Periodically assess effectiveness of the policies and procedures

Sample Policies and Procedures:

- Signed oaths of confidentiality for all affiliates
- Screens must remain private and should not be viewable from public areas.
- Desks should be clean
- Unattended computers and workstations should be locked or logged off
- All information managers or professionals providing information technology (IT) services must sign an Information Manager Agreement
- Mandate a minimum standard for passwords (e.g., passwords must contain numbers, special characters and a mix of upper and lower case letters)
- Require approval to be obtained from a clinic manager or lead physician prior to granting a user access to an electronic medical record (EMR) solution
- Require all new staff to complete a criminal background check
- Prohibit clinic personnel from downloading and installing software on clinic computers
- Prohibit disclosure of patient diagnostic, treatment and care information over the phone, even to an individual who claims to be the patient
- Required review of the EMR audit log by the clinic privacy officer every quarter
- Require laptops to be locked with a cable to a desk or post

Privacy Impact Assessments (PIAs)

Administrative safeguards are policies and procedures within the clinic that address the requirements for safeguarding health information.

The HIA requires that reasonable steps be taken to maintain administrative safeguards, and that maintenance goes beyond simply having safeguards in place.

To maintain administrative safeguards, a custodian must take reasonable steps to:

- Implement appropriate policies and procedures
- Educate and train affiliates on the policies and procedures
- Ensure affiliates comply with the policies and procedures
- Periodically assess effectiveness of the policies and procedures

Clinic PIA Tip

Section D, Project Privacy Risks and Mitigation, of your PIA contains a PIA Compliance segment that outlines the requirements clinic custodians must fulfill to meet HIA obligations.

Review this segment carefully to understand your clinic custodian HIA requirements.

Sample Policies and Procedures:

- Signed oaths of confidentiality for all affiliates
- Screens must remain private and should not be viewable from public areas.
- Desks should be clean
- Unattended computers and workstations should be locked or logged off
- All information managers or professionals providing information technology (IT) services must sign an Information Manager Agreement
- Mandate a minimum standard for passwords (e.g., passwords must contain numbers, special characters and a mix of upper and lower case letters)
- Require approval to be obtained from a clinic manager or lead physician prior to granting a user access to an electronic medical record (EMR) solution
- Require all new staff to complete a criminal background check
- Prohibit clinic personnel from downloading and installing software on clinic computers
- Prohibit disclosure of patient diagnostic, treatment and care information over the phone, even to an individual who claims to be the patient
- Required review of the EMR audit log by the clinic privacy officer every quarter
- Require laptops to be locked with a cable to a desk or post

Physical Safeguards

Physical safeguards are physical measures used to protect electronic health information from unauthorized access. Some examples of physical safeguards are:

Facility Access Control

- Limiting access to the building, clinic and storage areas

Facility Security

- Alarms and security cameras
- Doors and locks
- Lighting

- Identity badges for staff
- Property controls such as engraving equipment

Workstation Protection

- Log off or lock computers

Device and Media Control

- Control of portable storage devices (USB devices, hard drives, disks, etc.)
- Retention and disposal of information on devices
- Laptop locks

Other examples of physical safeguards include:

- Shredding documents that contain confidential information prior to disposal
- Placing fax machines and printers out of sightline and reach of public areas

Clinic PIA Tip

The Health Information Privacy and Security Manual included in your PIA provides detailed information about clinic safeguards:

- Policy 5, Information Handling, provides physical safeguard information that explains the steps your clinic must take to physically protect patients' health information records.
- Policy 7, Wireless Networking and Remote Access, provides administrative, physical and technical safeguards that must be implemented to protect clinic networking and remote access.
- The Risk Assessment Table outlines risks and mitigation strategies for internal and external physical security in your clinic.

Physical safeguards should be used in conjunction with technical and administrative safeguards. For example, workstations should have systems in place to automatically log off users if left unattended or unused for a short period of time. Proximity cards can automatically log off a user as soon as they leave the workstation.

Questions to Ask About Physical Security in Your Clinic

- Who has the pass-code for the clinic alarm system?
- Are laptop cables and locks used to prevent theft during clinic hours?
- After clinic hours, are laptops locked in a drawer or filing cabinet in a locked room?
- Are workstations secured during and after office hours?
- Are fax machines located in a secure area in the clinic, away from public view and reach?
- Are clinic staff required to confirm recipient's receipt of a fax?
- Are frequently used verified fax numbers pre-programmed into the fax machine to minimize human error?

It is also beneficial to review physical security with your clinic on a regular basis to ensure the safeguards are working, implemented properly and being used regularly as required by clinic staff.

Real Case Study

While a physician was on vacation, his laptop containing several months of billing data related to physician services was stolen from his office. The billing data identified patient names and associated services by billing code. Clinic staff contacted the police and the Office of the Information and Privacy Commissioner (OIPC) of Alberta to report the theft.

Consider:

- Was there a privacy breach?
- What could have been done to prevent this from happening?

Did a Privacy Breach Occur?
Yes, a breach occurred when the laptop was stolen. Once stolen, an unauthorized third party can potentially retain, use, access and/or disclose the health information contained on the laptop.

What Could Have Been Done to Prevent this from Happening?
Physical safeguards could have been put into place to prevent the theft, such as:

- Locking the door to the room or office in which the laptop was located
- Securing the laptop to another object, such as to a heavy table using a laptop lock cable
- Storing the laptop in a locked drawer or hotel safe

Technical safeguards could have also been used to prevent unauthorized parties from accessing and using the health information contained in the laptop. For example, the laptop hard drive could have been encrypted and password protected.

Module 3 Quiz

1. A new staff member is starting work at your clinic. Prior to accessing the EMR, which of the following needs to occur?	
☐	**a.** The new employee must review and sign a confidentiality oath.
☐	**b.** The clinic's privacy training must be completed by the new employee.
☐	**c.** A and B.
☐	**d.** None of the above.
2. Before leaving your clinic workstation computer, what are the necessary privacy procedures?	
☐	**a.** Leave the workstation and allow your computer to go into sleep mode.
☐	**b.** Ensure health information is not visible to the public.
☐	**c.** Lock your computer (e.g., use Ctrl + Alt + Del).
☐	**d.** B & C.

Module 3 Quiz – Answer Key

1. A new staff member is starting work at your clinic. Prior to accessing the EMR, which of the following needs to occur?
The answer is c. a & b. Before a new employee begins work at a clinic and accesses the EMR, they should review and sign a clinic confidentiality oath and complete the clinic privacy training. A criminal background check should also be completed prior to the individual being hired.
2. Before leaving your clinic workstation computer, what are the necessary privacy procedures?
The answer is c. b & c. Proper privacy procedures include ensuring health records are protected from public view and locking your computer so only authorized individuals can view health information records. Clinic staff members must be aware of and follow these procedures to ensure clinic health information records are protected.

Module 3 Summary

All clinic staff must be familiar with and implement the policies and procedures that have been documented in a clinic's PIA. Consistently implementing the administrative and physical safeguards help to protect the health information housed in a clinic.

Module 4: Technical Safeguards and External Threats

How can technology, combined with strong policies and procedures, help protect and control access to health information?

This module focuses on combining strong policies and procedures with robust technology to protect health information from external threats that include malware or spyware.

Clinic PIA Tip

The Health Information Privacy and Security Manual included in your privacy impact assessment (PIA) provides detailed information about clinic safeguards:

- Policy 5, Information Handling, provides physical safeguard information that explains the steps your clinic must take to physically protect patients' health information records.
- Policy 7, Wireless Networking and Remote Access, provides administrative, physical and technical safeguards that must be implemented to protect clinic networking and remote access.
- The Risk Assessment Table outlines risks and mitigation strategies for internal and external physical security in your clinic.

Technical Safeguards

What are Technical Safeguards?

Technical safeguards are technology and the policy and procedures for its use that protect and control access to electronic health information.

Examples of technical safeguards in electronic medical records (EMRs) are:

- Unique user identification
- Strong passwords
- Time-based, forced time-outs or log-offs
- Virus protection and firewalls
- Encryption of data
- Data backup and plans for service interruption
- Encrypted wireless Internet connections

Technical Safeguards in EMRs

Access controls in an EMR allow you to manage user accounts and privileges, usually in one (or more) of three ways:

- User-based access rights (secure)
- Role-based access rights (more secure)
- Context-based access rights (most secure)

Clinic EMR audit log reports should be reviewed every quarter and clinic privacy officers should know how to run these reports. If you need help, contact your vendor help support.

EMR consent management features are tools that allow you to mask or unmask certain data as per an individual's request. They can also anonymize data, which removes or replaces patient identifiers (such as name and address).

Questions to Ask About Technical Safeguards in Your Clinic

- When a computer or laptop has been idle for five minutes, does a screensaver automatically display and lock the computer?
- Are hard drives in computers and laptops encrypted?
- If you use a wireless network, is the transmission encrypted to the highest strength possible?
- Is your firewall and malware detection software up to date?

External Threats

Awareness of External Threats

Some examples of external threats are:

- Connecting remotely through unsecured wireless systems
- Malware (malicious software, designed to infiltrate or damage a computer system)
- Spyware (a type of malware that collects information, such as keyloggers)
- Irresponsible use of the Internet
- Internet-based file-sharing networks (when file-share networks such as Napster or Fastrack are installed, people may inadvertently share a file or download malware)

Risks from External Threats

- Identity theft
- Loss of information
- Information is shared with unauthorized individuals

To mitigate risks, provide regular training and refreshers on privacy and security to ensure staff are informed and aware of potential external threats. Computer system security should be reassessed by an IT professional when software or hardware is added to a system or hardware is being changed.

Questions to Ask About External Threats in Your Clinic

- Are users prohibited from using mobile data devices (such as iPods, flash memory sticks and external hard drives) on computers that access the EMR solution?
- Is the wireless network in the clinic encrypted using WPA or WPA2 standards?

Passwords

Using strong passwords lowers the risk of a security breach.

Clinic PIA Tip

Your PIA contains a Password Guidelines attachment in the Health Information Privacy and Security Manual.

Review these guidelines and ensure the minimum complexity requirements for password development are understood by all clinic employees.

Tips for Creating Strong Passwords

- Spell letters phonetically: the initials ABO can become AyBeeOh
- Use both upper and lower case letters
- Use at least one number
- Use at least one special character (such as the @, * or %)
- Do not begin or end the password with a number
- Make the password at least eight characters long
- Practise your new password on your keyboard
- Some systems allow the use of spaces in passwords

Tips for Maintaining the Security of Passwords

- Ensure passwords are not shared and, if shared, have each party change his/her password as soon as possible thereafter
- Require that passwords be changed on a regular basis
- Ensure passwords are not recorded in visible locations
- Ensure passwords are stored in an encrypted format and are not visually displayed when entered (e.g., the display is just *******)

Real Case Study

From IT World Canada (June 2007):
A video image of a woman providing a urine sample at a washroom in a methadone clinic in Sudbury, Ontario was accidentally intercepted by a backup camera in a vehicle that was driving by the clinic.

The contentious issue wasn't the presence of a surveillance camera in the washroom—as this was a methadone clinic, patients gave written consent to be monitored while providing urine samples. The crux of the investigation related to the clinic's use of an unsecured wireless surveillance system that was open to being—and was in fact—intercepted.

The clinic couldn't provide a satisfactory explanation of why it was using an unsecured wireless system—save to say the system was installed by a provider who had been recommended to them by the Sudbury police. "My sense is [they asked] very few questions of the service provider."

Consider:

- Who is responsible for ensuring the wireless network is secure?
- What could have been done to prevent this from happening?

Did a Privacy Breach Occur?
Yes, a serious breach occurred when the clinic had an unsecured wireless system.

What Could Have Been Done to Prevent this from Happening?
The clinic asked very few questions of the service provider and may have assumed the system was secure when it was not. Clinics must have a security assessment done each time new hardware or software are introduced into the clinic operating system.

Module 4 Quiz

1. "Barney1" is a strong password.	
☐	**a.** True
☐	**b.** False
2. Use of the audit log feature of an EMR system is a good way to monitor security.	
☐	**a.** True
☐	**b.** False
3. Unauthorized installation of software such as instant messaging or use of removable media can leave a clinic open to worms, viruses and hackers.	
☐	**a.** True
☐	**b.** False

Module 4 Quiz – Answer Key

1. "Barney1" is a strong password.
The answer is b. False A strong password includes numbers, symbols, upper and lowercase letters. Examples of strong passwords are "4pRte!ia@3" and "Ur2Fu$$ie." Using strong passwords lowers the risk of a security breach.
2. Use of the audit log feature of an EMR system is a good way to monitor security.
The answer is a. True The EMR reports in an audit log indicate the following about the accessed information: • Username and role • When and what information was accessed, updated and/or created • Any actions taken (including printing and masking/unmasking) Clinic privacy officers should know how to run these reports and should run them on a quarterly basis. If you need help running these reports, contact your vendor's help support desk.
3. Unauthorized installation of software such as instant messaging or use of removable media can leave a clinic open to worms, viruses and hackers.
The answer is a. True The policies and procedures surrounding the use of technology in a clinic help protect electronic health information and control access to it.

End of Module 4 Summary

Robust training, policies and procedures combined with professional IT support help to protect and control access to health information in the clinic setting.

Module 5: Notice and Consent for Disclosure

What roles do clinic staff, the clinic privacy officer, and the custodian have with respect to notice and consent for disclosure of health information?

This module focuses on understanding consent and disclosure as well as the roles and responsibilities of clinic staff members.

Providing Notice

What is providing notice?

When clinics collect individually identifying health information, the *Health Information Act* (HIA) requires that custodians must take reasonable steps to inform an individual of the:

- Purpose for which the information is collected
- Specific legal authority for the collection
- Title, business address and business telephone number of an affiliate of the custodian who can answer the individual's questions about the collection

A clinic notification should contain all three of the above required items. The requirement to provide notice is important because it:

- Recognizes an individual's right to know and understand the purpose of the collecting of their information
- Informs an individual about how their health information may be used
- Enables individuals to make informed decisions about providing their health information

A notice can be posted on the wall in a common area for patients to see (e.g., the waiting room or near reception).

Valid Consent Criteria

Valid Consent Criteria for Disclosure
The HIA and the Health Information Regulation has requirements on what is defined as valid consent criteria.

To be valid, consent must:

- Authorize a custodian to disclose the information
- Explicitly state what health information will be disclosed
- State the purpose(s) for disclosure
- Identify the person(s) to whom the health information will be disclosed
- Include patient acknowledgement
- Have an effective expiry date
- Include a statement indicating the patient can revoke their consent at any time
- Be in writing or an electronic format

Clinic PIA Tip
The Health Information Privacy and Security Manual in your PIA defines *consent* in Appendix 1, Definitions.

Review this definition carefully so you know what consent entails in applicable privacy legislation and clinic policies and procedures.

Rules for Disclosure

What are the Rules for Disclosure of Health Information?
The HIA says:

- Custodians may disclose a patient's health information to a third party if the patient has consented to the disclosure.
- Make sure you are disclosing to the correct individual or custodian.
- Be reasonably sure the information is accurate.
- Keep a log of the disclosures you make. A simple notation in the chart is acceptable.

Clinic PIA Tip
The Health Information Privacy and Security Manual in your PIA defines *consent* in Appendix 1, Definitions.

Review this definition carefully so you know what consent entails in applicable privacy legislation and clinic policies and procedures.

You may disclose without consent (although you are not required to do so by the HIA) to the following people:

- Continuing care and treatment providers.
- Health professional bodies, auditors and quality assurance committees.
- Researchers, subject to an ethics review.
- Entities authorized to obtain information or disclosures required by other legislation (e.g., courts or subpoenas).
- Family members in certain circumstances.
- Individuals or authorized representatives of individuals.
- Persons acting in the best interests of an incompetent individual.
- Police, when investigating a life-threatening injury to the individual.
- Any person, to avert or minimize an imminent danger.
- Another custodian, to prevent fraud or detect abuse of health services.
- Another custodian or successor of a custodian.

Note that the HIA itself does not require you to disclose, although in some cases other legislation does make disclosure mandatory.

There are also specific exceptions for disclosure without consent that apply to registration information and diagnostic, treatment and care information.

Routine Disclosure

Routine Disclosure: Release of Information
The disclosure of health information is part of a clinic's daily routine. Examples include patient's request of their own health information and requests for health information between custodians.

Some disclosures of health information require consent from an individual. This includes requests for disclosure to third parties such as insurance agents or legal representation.

Clinic PIA Tip
Policy 1, Right of Access, of the Health Information Privacy and Security Manual of your PIA provides information about an individual's access to their own health information.

Review this policy so you clearly understand the requirements and can implement them in your clinic procedures.

Section 41(1) of the HIA requires custodians to record the disclosure of patient information without consent. The record must include:

- The name of the person to whom the disclosure is made
- The date and purpose of the disclosure
- A description of the information disclosed

Because certain types of computerized health records, e.g., electronic medical records (EMRs) and electronic health records, typically track access to the information and log the user, date and time, the HIA has removed this requirement when disclosure is made through an EMR that has an audit function.

The EMR database must automatically maintain an audit log of the following:

- The user identification of the custodian who accesses the information
- The date and time that the information is accessed

Privacy Management Roles in a Medical Clinic

Physician (Custodian)

- Informs patients about disclosure of health information to conform to patient acknowledgement
- Provides information to patient about disclosure of health information and patient revocation rights
- Ensures all consent criteria have been met for consent to be considered valid
- Authorizes release of information
- Ensures each disclosure of written information has written consent
- Ensures each written consent is noted in the disclosure log

Clinic PIA Tip

Section B, Organizational Privacy Management, in your PIA provides a full review that includes privacy training and awareness resources for clinic roles.

Review this information so you can provide clinic staff with the resources they need to be aware of clinic privacy requirements and practices.

Privacy Officer (Affiliate or Designated Custodian)

- Assists in the development of privacy policies and procedures
- Ensures and enforces affiliate adherence to clinic privacy and security policies
- Ensures internal communication
- Receives and reviews breach notifications
- Responds to breaches
- Provides privacy training and support

The HIA requires custodians to establish a contact person as the clinic privacy officer. Privacy officers are responsible for ensuring their clinic complies with the act and assists with completion of the clinic PIA.

Clinic Staff (Affiliates)

- Adhere to clinic privacy and security policies
- Ensure consent received from patients is maintained and filed with patient chart in EMR or paper file
- Ensure each disclosure of written information has a written or electronic consent

All Staff are Responsible for the Following:

- Protecting the confidentiality of any health information they may have access to through the performance of their job duties
- Collecting, using and disclosing health information only in the performance of their job duties

- Reading and signing off on privacy and security policies and procedures
- Reporting privacy breaches to the privacy officer and/or privacy contact

Real Case Study

A clinic received a request for disclosure of health information from the son of a deceased individual who was a patient at the clinic. The son was estranged from the family and did not want to request information from the remaining parent. He was over 18 years of age and indicated he had a disease that he believed was hereditary. He requested that the clinic release the health information of his deceased parent.

Consider:

- If the custodian has an obligation to confirm the requestor's identity
- If the custodian has an obligation to confirm the deceased patient's wishes in regards to releasing health information

Could a Breach Occur?
If the custodian disclosed health information without applying due diligence, a privacy breach would occur.

What Could Prevent a Breach from Happening?
The custodian can release specific and relevant information under Section 35(1)(c), (d), (d.1), and (o) to the son, providing it is not contrary to the expressed request or wishes of the deceased individual. Additionally, the HIA allows for restricted disclosure to a deceased individual's descendant if disclosure is necessary for providing a health service to the descendant (Section 35(1)(o)).

Any request for disclosure warrants the following actions:

- Check the patient's file for any expressed wishes or any non-disclosure statements
- Verify the identity of the requestor
- Develop and follow proper clinic policies and procedures to deal with health information access requests
- Stamp "copy" on all hard copies of any health information disclosed
- Log all disclosures of health information in the clinic's disclosure log

There are exceptions to the "expressed wish" clause outlined in the HIA (e.g., in cases of providing health service to descendant or a police request).

Module 5 Quiz

1. A physician can disclose health information to a patients' insurance company without the patient's written consent.	
☐	**a.** True
☐	**b.** False
2. A written notice is not necessary to post in the clinic regarding the purpose for collecting personal health information; providing verbal explanations, when asked are all that is necessary.	
☐	**a.** True
☐	**b.** False

Module 5 Quiz – Answer Key

1. A physician can disclose health information to a patients' insurance company without the patient's written consent.
The answer is b. False Custodians can disclose a patient's health information to a third party only if the patient has consented to the disclosure.
2. Use of the audit log feature of an EMR system is a good way to monitor security.
The answer is b. False A posted written notice is necessary. Written notice must be provided to inform patients about the purpose for collecting personal information. Written notice can be provided by posting a sign in a common area such as a waiting room or in reception. Hard copies should also be available to patients upon request.

End of Module 5 Summary

Ensure that all staff, students, volunteers and contracted personnel are aware of their duties, roles and responsibilities under applicable privacy legislation. It is a best practice to enforce clinic policies and procedures, provide training and obtain signed oaths of confidentiality to ensure that all clinic staff comply with the HIA.

Review and Best Practices

Combining robust administrative safeguards, strong physical safeguards and complete technical safeguards will help to ensure that health information is accessed, collected, used and disclosed, and protected in compliance with Alberta's *Health Information Act* (HIA).

This section quickly reviews the previous five modules and provides some examples of best practices policies and procedures used in many clinics.

Module 1 Review: Health Information

When you collect, use or disclose health information, it is done on a need-to-know basis, disclosing the least amount of information necessary with the highest level of anonymity possible, within your legal authority. You must request consent as required and take reasonable steps to protect that health information.

It is a clinic responsibility to implement, review and train staff on privacy, security and confidentiality policies and procedures.

Module 2 Review: Privacy, Security and Confidentiality

Clinic custodians and affiliates must follow the privacy, security and confidentiality requirements of the HIA. These requirements are upheld by the HIA offences and penalties documented in Section 107.

Become familiar with these requirements so you can help prevent privacy breaches from taking place in your clinic.

Module 3 Review: Administrative and Physical Safeguards

A clinic's administrative safeguards—its policies and procedures—are outlined in a clinic's privacy impact assessment (PIA). These policies and procedures will address maintaining the security and privacy of health information. The PIA should be reviewed and updated on an annual basis.

Signed oaths of confidentiality combined with regular training and support help to facilitate compliance with the HIA.

Physical measures such as locks and access controls, also outlined in a PIA, require an annual review and update as well.

Module 4 Review: Technical Safeguards and External Threats

Technical safeguards are best maintained by an information technology (IT) professional. Clinic staff need to be made aware of external threats and how clinic policies and procedures protect and control access to health information.

When hardware or software is introduced to a clinic's operating system the PIA should be reviewed and may need revisiting.

Module 5 Review: Notice and Consent for Disclosure

A physician's office must provide written notice about the collection of health information.
The principles of disclosure are:

- You can disclose a patient's health information with consent.
- Make sure you are disclosing to the correct individual or custodian.
- Be reasonably sure the information is accurate.
- Keep a log of the disclosures you make. A simple notation in the chart is acceptable.

A privacy officer in the physician's office supports the other affiliates and the custodian in meeting the requirements of the HIA.

Best Policies and Practice

- Never share your user name and/or password. You are responsible for all access under your security credentials.
- Only access health information necessary to fulfill your job responsibilities, and keep this information confidential.
- Never access information for non-business purposes (such as your own or a relative's EMR record).
- Always log off your EMR and lock your computer when you step away from your workstation. To log off a Windows computer, use the ctr + alt + del keystroke. To log off a Macintosh computer, use the shift + command + Q keystroke.
- When printing information from a patient's EMR, follow your clinic policy in the use, storage and disposal of these print-outs.
- Regularly review and update your privacy and security policies and procedures.
- Regularly train staff on privacy.
- Use the technical features of your EMR that offer the highest level of privacy and security, such as context-based user access, audit logs and automatic log-off systems.
- Have information technology (IT) professionals maintain the technical safeguards of your office system.
- Ensure IT professionals providing services to your clinic sign an Information Manager Agreement (IMA).
- Ensure all affiliates sign an oath of confidentiality.
- Update your signed oaths of confidentiality regularly.
- Conduct periodic privacy and security self-assessments.

Final Quiz

1. Under the right to access, a clinic employee has the right to access their own medical record directly, using job-related access in their clinic EMR.	
☐	**a.** True
☐	**b.** False
2. Patients can look at their own charts whenever they want.	
☐	**a.** True
☐	**b.** False
3. How can you protect your patients' health information from unauthorized individuals?	
☐	**a.** Log off computer terminals and/or have password protected screen savers.
☐	**b.** Don't give out your computer logon and/or password to anyone.
☐	**c.** Position printers and computer monitors so that information is not accessible or viewable by unauthorized viewers.
☐	**d.** All of the above.
4. Your brother sends you an email at work with a screen saver he says you would love. What should you do?	
☐	**a.** Download it to your computer, since it's from a trusted source.
☐	**b.** Forward the message to other friends to share.
☐	**c.** Call your IT help desk and ask them to help you install it.
☐	**d.** Delete the message.
5. Which workstation security safeguards are clinic staff responsible for using and/or protecting?	
☐	**a.** User ID.
☐	**b.** Password.
☐	**c.** Log-off Programs.
☐	**d.** Lock up the office and/or work areas (doors, windows, laptops).
☐	**e.** All of the above.

6. When sending information by fax, you should:	
☐	**a.** Verify the number you are faxing to.
☐	**b.** Send it without a cover sheet because they know it's coming.
☐	**c.** Verify the recipient's identity and validate the purpose of the request.
☐	**d.** Both A & C.
7. You decide to add some voice-recognition software to your office system. Your next steps may be: i) Have the IT professional install it for you; ii) Notify the POSP office of an amendment to your privacy impact assessment (PIA); iii) Have the IT professional sign an Information Manager Agreement in case of exposure to any health information during their work. Identify the correct order of the steps:	
☐	**a.** i, ii, iii
☐	**b.** ii, iii, i
☐	**c.** iii, i, ii
8. One of your clinic staff used Netcare to view their daughter's lab results. This is an acceptable use of Netcare, since she is the child's parent and legal guardian:	
☐	**a.** True
☐	**b.** False
9. When approached by a police officer requesting patient information, you should:	
☐	**a.** Hand it over, because law enforcement is entitled to this information.
☐	**b.** Indicate that you need the request in writing and then you can give them a copy of what they need.
☐	**c.** Consult your clinic privacy officer before releasing anything.
10. Choose the correct statement:	
☐	**a.** As an employee, you are permitted to access any patient's record for whatever you want.
☐	**b.** As an employee, you can use your EMR system or Netcare to access your own health information.
☐	**c.** As an employee, you are permitted to access a patient's health information if your job duties/responsibilities require you to do so.
☐	**d.** If you are an affiliate, you cannot be personally responsible for violations, only the custodian can be fined or penalized.

Final Quiz – Answer Key

1. Under the right to access, a clinic employee has the right to access their own medical record directly, using job-related access in their clinic EMR.

The answer is b. False
Clinic employees may not access any electronic medical records for a non job-related reason, even their own. All patient(s), even employees, must request access to their own record, and must request a copy from the custodian.

2. Patients can look at their own charts whenever they want.

The answer is b. False
The patient must request permission from the custodian (physician) to view their chart. The custodian may charge a fee to make a copy of the record.

3. How can you protect your patients' health information from unauthorized individuals?

The answer is d. All of the above
Ensure workstations have the proper settings in place to display the password protected screen saver after a short period of idle time. When a user is leaving a workstation unattended, good practice is to lock the workstation by using Ctrl + Alt + Del buttons simultaneously and selecting the option to lock the computer. If someone suspects their password has been compromised, request they change their password immediately and notify the privacy officer. Fax machines should also be positioned to be inaccessible by unauthorized individuals.

4. Your brother sends you an email at work with a screen saver he says you would love. What should you do?

The answer is d. Delete the message.
Delete the message immediately; do not attempt to open the email message. Email attachments should be opened with extreme caution as they can contain computer viruses.

5. Which workstation security safeguards are clinic staff responsible for using and/or protecting?

The answer is e. All of the above
Applying all of these safeguards will help ensure the security of health information throughout your clinic.

6. When sending information by fax, you should::

The answer is d. Both a and c.
Including a fax cover sheet that contains notification on the following is standard best practice:

- Confidentiality of the information contained in the fax.
- Instructions on what should be done if the fax is sent to a wrong number.

Use pre-programmed, validated fax numbers as often as possible. Calling the recipient to confirm the fax has been received by the correct party is also best practice

7. You were just made aware that one of your clinic staff sent a fax containing individually identifying health information to an auto body shop. Check all the actions you should take from the list below:

The answer is b.
First, notify the POSP office of an amendment to your PIA to receive templates. An update to your PIA should the be submitted to the OIPC before any new installation begins. The IT professional responsible for implementing software must sign an Information Management Agreement prior to reviewing data in preparation for implementation.

8. If a patient's husband calls for the results of his wife's pregnancy test and he provides you with her name, date of birth, address and phone number over the phone, you can tell him the results of her test.

The answer is b. False
Test results are considered diagnostic, treatment and care information. In this case, the physician or clinic staff member should not disclose the information to the husband without consent of the patient.

9. When approached by a police officer requesting patient information, you should:

The answer is c: Consult your clinic privacy officer before releasing anything.
The clinic privacy officer should handle these requests. Disclosure may be made to the police for the purpose of investigating an offence involving a life-threatening personal injury to a patient and if it is not against the express wishes of the patient. Note that disclosure may also be made to the police for the purpose of avoiding imminent danger to the health and/or safety of any person.

10. Under the HIA, when it comes to health information, clinics are responsible for the actions of their third-party vendors and contractors such as their EMR provider and shredding or transcription companies.

The answer is c. As an employee, you are permitted to access a patient's health information if your job duties/responsibilities require you to do so.
Access to patient health information should be on a need-to-know basis.