Alberta Health Services

Annual Continuing Education (ACE)

(Print version)

Information Privacy and I.T. Security and Compliance

Information Privacy and IT Security & Compliance

The information in this module in addition to the Information Privacy and IT Security & Compliance Awareness video meets the education requirements of HIA and FOIPP legislation for all AHS employees.

Every AHS employee is expected to follow the Freedom of Information and Protection of Privacy Act (FOIPP), the Health Information Act (HIA), the AHS Code of Conduct and AHS Information and Technology Management policies when collecting, using, accessing, disclosing and disposing of information. The following module provides an overview of these two acts as well as actions staff must take to safeguard confidentiality and privacy of information.

Time needed to complete module: 40 minutes

Please retain your completed and self-corrected quiz for your records and to provide to your manager, if they require you to do so.

* *An alternate e-learning version of ACE is available on MyLearningLink.*

Prerequisite/Pre-reading

Required
Review Information & Privacy and IT Security & Compliance Awareness video on Insite: http://insite.albertahealthservices.ca/1213.asp

Optional
Review resources available on Insite:

- http://insite.albertahealthservices.ca/corporate-policies.asp.
- http://insite.albertahealthservices.ca/3141.asp

Overview

At Alberta Health Services (AHS), it is our responsibility to respect confidentiality and privacy. This means protecting the information of our patients, clients, co-workers and AHS organizational information. Every employee is expected to follow the Freedom of Information and Protection of Privacy Act (FOIPP), the Health Information Act (HIA), the AHS Code of Conduct and AHS Information and Technology Management policies when collecting, using, accessing, disclosing and disposing of information.
The following module provides an overview of these two acts as well as actions staff must take to safeguard confidentiality and privacy of information.

Objectives

By the end of this module you will be able to:

- Define Privacy, Confidentiality and Information Security
- List who is responsible for protecting health and personal information in AHS
- Describe the purpose of the Freedom of Information and Protection of Privacy Act and the Health Information Act
- Describe how to protect the privacy of health and personal information and acceptable use of information technology (IT).

Did you know?
In 2007 a medical office clerk from Calgary was fined $10,000 for improperly accessing the medical records of another person in contravention of the HIA.

What is Privacy?
Privacy is the right of the individual to be left alone, to be free from interference, from surveillance and from intrusion.

What is Confidentiality?
Confidentiality is our organizational obligation to protect the information given to us, to maintain the secrecy of the information, and to ensure it is collected, used, accessed and disclosed only as authorized by law.

What is Information Security?
Information Security is the physical, technical, or administrative arrangements that our organization uses to prevent information from being lost, altered or disclosed without authority.

Tip… Use a strong password that will not be easy for others to figure out. Try using the first letters from a favorite song line, or adding punctuation marks.

Who Is Responsible?
Everyone is responsible for protecting the health and personal information of our patients, clients and co-workers as well as Alberta Health Services business information.

This includes:
- health service providers
- employees
- volunteers
- students
- contractors
- persons acting on behalf of AHS

Health Information Act and Freedom of Information and Protection of Privacy Act

Two pieces of privacy legislation in Alberta guide the way AHS collects, uses, discloses and protects information. These include:
1. Freedom of Information and Protection of Privacy Act (FOIPP)
2. Health Information Act (HIA)

The Freedom of Information and Protection of Privacy Act, otherwise known as FOIPP, provides rules for collecting, using and disclosing personal information. Personal information can include things such as name, contact information, birth dates, and employment information.

The Health Information Act provides those same types of rules as FOIPP for health information, such as a person's registration or diagnostic, treatment and care information. The HIA also outlines responsibilities for the protection of health information.

Both FOIPP and the HIA provide a method for individuals to access and correct their own information and AHS organizational information and also provide a complaint / dispute resolution process under the Office of the Information & Privacy Commissioner of Alberta.

Key Privacy Principles

You must collect, use and disclose information based on the three privacy principles:

- **need to know (not nice to know),**
- **least amount of information required to do your job, and highest level of anonymity.**

Did you know?
You are not permitted to access your own information or that of friends, family members, or co-workers (including both paper or electronic records). Audits of information access are reviewed and inappropriate access may result in disciplinary action.

Collection, Use and Disclosure of Information

Collection, use and disclosure of information must be limited to the amount that is required to carry out your roles and responsibilities.

The concept of **collection** means to gather acquire or obtain information.

The concept of **use** means the internal sharing of health information within AHS or its affiliates.

The concept of **disclosure** means the external sharing of health information with those outside of AHS.

Did you know?
An individual may expressly ask AHS to limit how their health information is disclosed. These wishes must be considered when making decisions about disclosing the information.

An individual may expressly ask AHS to limit how their health information is disclosed. These wishes must be considered when making decisions about disclosing the information.

Need to Know Principle

You should only collect, use or disclose information if doing so is necessary for carrying out your job duties. Your ability to access information does not give you the right to access information not required for your job.

Least Amount of Information Principle

Not all information about an individual is relevant or required in all situations. You are required to collect, use, and disclose the least amount of information you require to carry out an intended purpose.

Right of Access

Individuals have the right to request access and corrections to their own personal or health information from AHS. The public can also request access to records and organizational information in the custody of AHS.

There are circumstances where AHS is required by the HIA or FOIPP to withhold information, or when AHS can choose to withhold information.

Although you have a right to request access to your personal and health information, this does not give you the right to access the information by looking it up yourself on an electronic system or in paper records.

When you, a family member, friend, co-worker, client or patient would like to view or obtain copies of personal or health information, the approved request process outlined in AHS policy must be followed.

Reflect: What kind and amount of information do you really need to know to perform your job? How much of it is confidential?

Duty to Protect

Treat all personal and health information as if it was your own. It is your duty to protect confidential information.

Report all privacy and security breaches

- Misdirected faxes, mail, emails
- Lost records
- Inappropriate access to health records or surfing health application systems
- Taking pictures inappropriately (other employees, patients, etc.)

Did you know?
Posting of personally-identifiable health information on social media sites (facebook, Twitter, YouTube, MySpace) contravenes AHS policies and may result in disciplinary action.

- Emailing health information should be avoided. If you must email health information external to AHS, ensure you use AHS encryption.

See the Information Technology Acceptable Use policy Protection and Privacy of Health and Personal Information policy for more information.

Alberta Health Services Code of Conduct and Information & Technology Management Policies

Everyone is responsible for understanding and complying with Alberta Health Services Code of Conduct and Information & Technology Management policies. These policies include:

- IM-01 Access to Information (Physical, Electronic, Remote)
- IM-02 Contractor Requirements for Security of Information and Information Technology Resources
- IM-03 Transmission of Information by Facsimile or Electronic Mail & Appendix “A”
- IM-05 Protection and Privacy of Health and Personal Information & Appendix “A”
- IM-06 Information Technology Acceptable Use & Appendix “A”
- IM-07 Records Management Policy & Procedures

These policies can be found on Insite http://insite.albertahealthservices.ca/corporate-policies.asp.

Failure to follow the provisions of the legislation and/or Information & Technology Management policies may be considered grounds for disciplinary action, up to and including dismissal.

Tip: Help keep confidential information secure by keeping your work area clear. If you are going to be away from your work area overnight or for an extended period of time, lock up confidential information in a cabinet, drawer or other storage area.

Transmitting Information

Privacy legislation requires that information is protected from any foreseeable risk. This includes making sure any information sent by **fax** or **email** is secure while it is being transmitted.

Requirements for Faxing Information

1 Use pre-programmed numbers (speed dial) when possible
2. Visually check and verify the number dialed before faxing.
3. Always use the standard AHS cover sheet containing a confidentiality statement/disclaimer.
4. Never include individually identifiable or confidential information on a cover sheet.
5. Remove sent or received documents from fax machine as soon as possible.
6. Print a transmission log report.

Requirements for Emailing Information

1. Email sent to addresses external to AHS are not secure and can be intercepted or forwarded to additional recipients. Any confidential email sent to a non-AHS email address must be encrypted.
2. Visually check all email addresses prior to sending to ensure the recipient is correct.
3. Review email threads before forwarding or replying to emails – always send the least amount of information

Encrypting Email

AHS employees and representatives have the responsibility to ensure that any sensitive information sent to an external recipient is encrypted.

To learn how to encrypt e-mail and for more information please visit the AHS Email page on Insite. http://insite.albertahealthservices.ca/3141.asp

Transporting information

When you carry information with you, either inside an AHS facility or outside an AHS facility, you are responsible for making sure the information is secure and protected from loss or theft. It is also important to make sure that any information sent by internal or regular mail or courier is properly packaged and sealed.

When sending information by mail, always consider the most appropriate method (e.g., inter-facility mail, registered mail, courier) and include complete and legible address information. It is also best practice to include the address and name of the sender in the event that the information is undeliverable.

Requirements for Transporting Information

1. Do not remove original records from an AHS facility unless absolutely necessary and approved by your manager.
2. Only take the minimum amount of information with you needed to perform the task.
3. Secure information in a closed, non-transparent container (e.g., briefcase) and attach your contact information.
4. Keep the information under your direct control at all times and do not leave it unattended in a vehicle.
5. Information should not be visible at any point during transport.

What do you do if you suspect there has been a privacy breach or information security incident?

If you know or suspect that there has been an unauthorized collection, use, disclosure, access to or disposal of information, take immediate steps to reduce the risk of further harm (e.g., secure the affected document or system) and report it to your supervisor. Also notify the Information & Privacy office immediately by contacting privacy@albertahealthservices.ca.

An information security incident involves a weakness or malfunction of IT infrastructure that could affect the security of information. Notify IT Security & Compliance of security incidents by contacting securityincident@albertahealthservices.ca.

Summary

Now that you've reached the end of this module, you should be able to recall that:

- Information security includes the arrangements made to safeguard and protect company information.
- Everyone is responsible for protecting the health and personal information of patients, clients and co-workers.
- The Health Information Act and Freedom of Information and Protection of Privacy Act are two pieces of legislation that guide AHS's security protocols.
- Failure to follow the provisions of the legislation and/or information policies can be grounds for disciplinary action up to and including dismissal.

Quiz answers on page 11

Questions for Review:

1. Volunteers and contractors do not have the same level of responsibility as employees for protecting the health and personal information of our patients.
   - ☐ True
   - ☐ False

2. Which of the following types of information must be protected:
   a. Employees' personal information
   b. Patients' health information
   c. AHS' business information
   d. All of the above
   e. None of the above

3. FOIPP provides rules for collecting, using and disclosing personal information, whereas HIA provides rules for collecting, using and disclosing health information.
   - ☐ True
   - ☐ False

4. Personal or Health Information?
   Indicate whether the following are personal or health information:

   a. Employee work schedules or on-call lists.
   - ☐ Personal Information
   - ☐ Health Information.

   b. Laboratory or diagnostic imaging test results.
   - ☐ Personal Information
   - ☐ Health Information.

   c. The name, business title or profession of a health service provider.
   - ☐ Personal Information (If the information is related to a health service provided to an individual (e.g., the name of a physical therapist who provided treatment to a patient), it is the health information of that individual.)
   - ☐ Health Information.

5. Information Use or Disclosure?
   Indicate whether the following situations are examples of use of information or disclosure of information.

   a. Faxing a patient's discharge summary to their family physician at the physician's clinic.
      - ☐ Disclosure
      - ☐ Use
      - ☐ Collection

   b. Providing relevant health information about a patient to a co-worker who is also responsible for the patient's direct care.
      - ☐ Disclosure
      - ☐ Use
      - ☐ Collection

6. Protecting Information
   Indicate whether the following are true or false.

   a. Only patient information is confidential.
      - ☐ True
      - ☐ False

   b. Only those involved in direct patient care are responsible to protect the confidentiality of information.
      - ☐ True
      - ☐ False

   c. AHS uses administrative, physical and technical safeguards to protect information.
      - ☐ True
      - ☐ False

Answers: ***1.*** *False* ***2.*** *D. All of the above* ***3.*** *True*
4. *a. Personal Information b. Health Information c. Personal Information*
5. *a. Disclosure b. Use* ***6.*** *a. False b. False c. True*