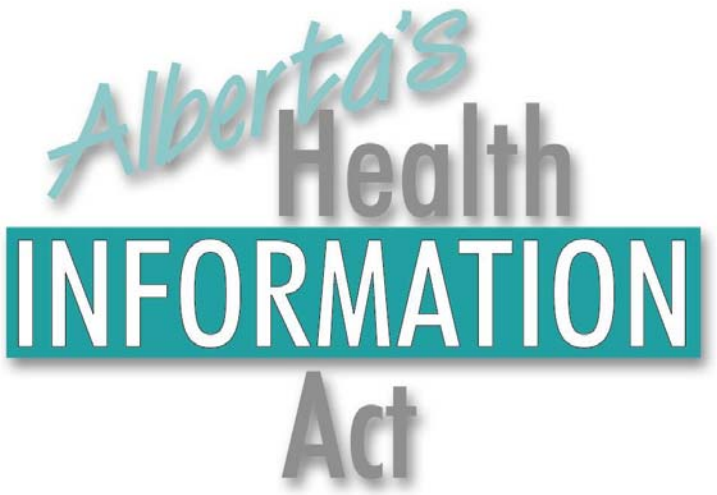

Online Training

Duty to Protect Health Information

Department of Medicine
University of Alberta

Last updated: July 19, 2011

Duty to Protect Health Information

Custodians must:

- Take reasonable steps to protect the health information in their custody.
- Designate an affiliate in charge of the security of health information. This would most likely be his or her secretary.
- Identify, and maintain, a **written record** of all:
  1. Administrative Safeguards;
  2. Physical Safeguards; and
  3. Technical Safeguards.

Duty to Establish or Adopt Policies and Procedures

- Custodians must establish or adopt policies and procedures to ensure compliance with the Act.
- This helps demonstrate due diligence with respect to the Act should there be any complaints.

Safeguards

Custodians must protect against reasonably anticipated threats or hazards to the security or integrity of health information. They do this by having three types of safeguards in place:

1. Physical safeguards;
2. Administrative safeguards; and
3. Technical safeguards.

1. Administrative Safeguards

Administrative safeguards are policies and procedures that ensure the safety of health information.

Some important administrative safeguards:

- Using extreme caution when giving out information over the phone.
- Restricting access to health information to those with a ***need to know***.
- Ensuring that a Confidentiality Agreement is signed by all people with access to health information.
- When no longer working for the custodian the employee should be debriefed with respect to maintaining confidentiality, access privileges should be revoked and security-related items must be retrieved (eg.: badges, etc.).

- If health information must be given verbally, ensure that nobody can overhear the conversation.
- All staff need to be trained on the custodian's policies and procedures, and a record maintained of training dates. Policies and procedures should be reviewed on an annual basis.
- Policies and procedures should be updated regularly with dates recorded.
- Be aware of the wishes of the patient regarding confidentiality.
- Shred documents with health information immediately instead of storing them for later.

For faxes:

- Always use a fax cover sheet specifying the sender and receiver.
- Include a confidentiality statement on all faxes. For examples of confidentiality statements, see:
- Do not fax anything you would not be comfortable discussing over the phone.

For faxes (continued):

- Program frequently used numbers into the fax machine and keep up to date, confirm numbers on a regular basis, record the dates this is done.
- Confirm the fax number prior to sending and confirm it has been entered correctly by checking the display window.
- Determine how frequently the fax machine should be checked for faxes, and/or appoint someone to collect faxes.

For faxes (continued):

- Establish policies for dealing with faxes with no addressee specified.
- Security precautions should be taken for faxes received after normal office hours
- If you are using a fax modem, confirm other users of the computer system cannot get access to the fax without a password.

For email:

- Email should be used with extreme caution. Try not to email identifying health information, as email systems are ***not*** secure.
- If email must be sent, ensure that it is properly secured by using encryption methods.
- Like faxes, emails must have a confidentiality statement attached to the bottom.

2. Physical Safeguards

Physical safeguards ensure that health information is kept physically safe. If the public has access to your area, you need to ensure that people without a need to know do not have access to health information.

Some important physical safeguards:

- Physicians should dictate behind closed doors.
- Keep rooms and files locked when unoccupied.
- Keep files, laptops, portable devices, and USB drives containing health information in locked cabinets when not in use.
- Protect from fire: Equip storage rooms with smoke detectors and fire alarms.

- Do not leave files out containing health information when away from your desk. If they need to be out, hide the name from passers-by.
- Keep monitors out of sight from the public or passers-by.
- Position fax machines so that they are inaccessible to non-staff.
- Used locked bins for shredding.
- Physicians should dictate behind closed doors.

- Maintain a current, written record of who has keys/codes to areas where patient files are kept.
- Do not make unnecessary stops or set files down when transporting to/from the clinic and keep them out of sight.
- In clinics do not leave files in the doors so that the names are showing to passers-by.

3. Technical Safeguards

Technical safeguards apply to things like computers and portable devices.

Some important technical safeguards:

- Back up files regularly.
- Safe files to backed-up networks instead of locally on your machine.
- Use non-obvious passwords.
- Lock your computer when stepping away from your desk.

- Format old computers and disks when disposing of them. Deleting files is not sufficient.
- Use USB drives with two-level security (password protection and encryption).
- Keep virus protection up to date.
- When storing and transmitting particularly sensitive information make sure that it’s properly encrypted.

Policies and Procedures

- Policies and procedures basically include the Record of Safeguards, as well as the steps for processing requests for information (these steps are covered in other slide presentations). You can use one document to cover both.
- A policy and procedures template is available from the Department of Medicine website at:

http://www.medicine.med.ualberta.ca/Library/Documents/staff/hia/02-policiesprocedures.pdf

Why are policies and procedures necessary?

- Having policies and procedures in place shows ***due diligence*** on the part of the custodian.
- If there should be a complaint/breach of the Act, the investigator will look at:
  - What policies and procedures were in place to deal with issues of privacy and security and comply with the Act; and
  - Whether or not the policies and procedures were followed.

- It is the duty of every custodian to conduct a ***threat assessment*** of his or her office, clinic, and procedures to determine what are reasonably anticipated threats or hazards to the integrity, confidentiality and security of health information.
- They then need to determine what are reasonable steps that can be taken to prevent those reasonably anticipated threats or hazards to the integrity, security and confidentiality of the health information.

Last Slide in this Set

Congratulations! You can now move on to the next set of slides - ***Disclosing Health Information With Consent.***