Department of Medicine
HIA Guidelines for Support Staff

As support staff, your actions are held accountable to the Health Information Act (the "HIA"). You are considered an "affiliate" under the HIA. The physician that you work for is considered a "custodian".

As an affiliate, you have several responsibilities that relate to the Act. First and foremost, your primary responsibility is to follow safeguards to protect confidential health information. You are also required to maintain notations of disclosures of health information.

Your physician must appoint an affiliate who is responsible for the overall security and protection of health information under his or her control. You may find that you are the appointed person! If this is the case, you will be responsible for creating your office's privacy safeguards, ensuring that everybody follows them, and assessing them periodically. You will also be the contact person for any requests for access or amend health information and answer any of the patients' questions or concerns about their personal information.

Safeguards

A custodian must protect against reasonably anticipated threats or hazards to the security or integrity of health information or the loss, unauthorized access, use, disclosure or modification of health information. They do this by having three types of safeguards in place:

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

Custodians must identify and record these three safeguards - they may do this themselves or they may ask the appointed affiliate to do this for them. Either way, it is your responsibility to follow the safeguards at all times in your day-to-day duties.

1. Physical Safeguards

Physical safeguards ensure that health information is kept physically safe. The safeguards that need to be taken will depend partly on where your office is located and how much traffic is in your area. If the public has access to your area you need to be particularly careful to make sure people who do not need to see health information do not have access. Some important physical safeguards include:

- Keeping rooms locked when unoccupied.
- Equipping storage rooms with smoke detectors, fire extinguishers, and fire alarms.
- Maintaining a current record of key holders for access to offices and storage areas.
- Use of signs such as "Authorized Staff Only" if the public has access to areas in or around your office.
- Keeping files, laptops, and portable devices such as USB drives and PDAs containing identifiable personal information in locked filing cabinets when not in use.
- As much as possible, keeping your desk clear of files when you are away from your desk. If you do need to keep files on your desk, keeping identifiable personal information on the files out of sight.
- Keeping computer monitors out of sight from the public or passers-by. If your computer is in an open area, consider obtaining a privacy screen for your monitor.
- Positioning fax machines so they are inaccessible to non-staff.
- Locating in-boxes, cubby holes and mailboxes so they are inaccessible to non-staff.
- If you are transporting patient information, ensuring its safe transport by not stopping along the way. Keep all files and devices being transported out of sight. If you are bringing work home with you in the evening, keep all information stored in a secure area where others do not have access to the information.
- Use locked bins for confidential shredding.

2. Administrative Safeguards

Administrative safeguards are policies and procedures that ensure the security of health information. Important administrative safeguards include:

- Ensuring that only the least amount of information necessary for the intended purpose is collected, used and disclosed.
- Restricting access to health information to staff who require access to the information in order to perform their job duties. This involves restricting access to information to those with a "need to know". This means that access to information should only be allowed if it relates to their specific duties and if the information relates only to the patient that they are responsible for or providing care to.
- Ensuring that confidentiality and security of information is addressed as part of the conditions of employment for new staff, and is written into job descriptions and contracts.
- Monitoring staff for compliance with privacy and security policies and procedures.
- Making sure that a Confidentiality Agreement is signed by all staff, students, volunteers, and contracted personnel (e.g., janitors, temporary staff, etc.).
- Ensuring that patients and visitors are accompanied by a staff member to private or semi-private areas such as examination rooms and/or physician offices.
- Reporting all privacy compliance issues and security breaches to the physician or appointed privacy contact.
- Ensuring all staff members are trained on the HIA. The Department of Medicine has online HIA training that can be found at: http://www.medicine.med.ualberta.ca/Home/Staff/HIA/training.cfm.
- Ensuring that confidential information is not transmitted verbally if conversations can be overheard or intercepted.
- Using extreme caution when giving out information over the phone:
    - Do not give out patient information over the phone unless the individual is *authorized* to receive the information AND you are reasonably sure of the *identity* of the individual.
    - If it is the patient calling, but you do not recognize him or her, check your call display, ask him/her to provide two pieces of information such as their date of birth, name of their family physician, or postal code, AHC # or other information, or tell them you will call them back at their home or work number if they are not calling from one of those numbers.
    - If it is a family member, ask their relationship and confirm with the patient, if possible. Check the patient file to see if the caller is listed as family. You would only be discussing appointments, referrals or booking lab tests, otherwise the physician should talk to the caller. If the patient gives permission to talk to a family member, make a note in the file regarding what type of information you can disclose to them.
- Using care when faxing patient information. See "Guidelines on Fax Transmission" (http://www.oipc.ab.ca/ims/client/upload/Guidelines_on_Facsimile_Transmission.pdf).
- Shredding documents with patient names immediately instead of storing them to be shred later.
- Using caution if the patient is a teenager - they may not necessarily want information given to their parents. A person under the age of 18 could be considered a "mature minor", if they understand the nature of the right or power and the consequences of exercising the right or power. Parents do not automatically have a right to information on their children unless the patient is too young to understand.
- Being aware of the express wishes of the patient regarding confidentiality. Ask your physician to keep you informed if the patient who specifically states that they do not want anyone to know about their health or that they do not want a particular family member to know about their health.
- Knowing how to handle requests from other physicians. If a medical clinic is calling for information about a patient, and you are not familiar with the physician or the clinic, ask them to fax the request on letterhead. Ideally, they should include the patient's consent with the request. If a physician is requesting information for the purpose of providing a health service, consent is not required, but they should obtain it and provide it if possible.

3. Technical Safeguards

Technical safeguards apply to things like computers and portable devices. They include:

- Backing up files on a regular basis.
- Saving your files to backed-up network drives instead of locally on your own machine.
- Using non-obvious passwords, and changing them regularly. Don't write your passwords down, post them publically, or share them with others.
- Remembering to either lock your computer or log off if leaving your desk – even if you are gone for only a moment.
- If appropriate, the use of security/privacy screens. This way, the computer monitor can only be read when you are directly in front of it.
- When disposing of old computers and disks, formatting the hard drive and the disks.
- If you need to use a USB drive, using one with two-level security, i.e. both password protection and encryption. Lock it away when not in use.
- Keeping up-to-date virus protection.
- Not sending out patient information via email, as it is typically unsecured. If it needs to be emailed, make sure that it has adequate encryption.

Making and Maintaining Notations of Disclosures of Health Information Made

It is important to know the difference between using health information, and disclosing health information. *Using* refers to sharing health information *within your office or clinic.* If a patient's health information is given to someone *out of the office or clinic,* including to another physician for the purpose of providing continuing care, it is considered a *disclosure.*

Custodians are required to keep a record of all disclosures made. This record can be requested by the patient or an authorized individual at any time and must be kept for ten years after the disclosure. However, most disclosures are in the form of follow-up letters to family physicians and include the name of the family physician and the date they are written. As long as these letters are kept in the patient file this is sufficient notation of the disclosure.

When a physician is disclosing individually identifying health information to someone who is *not* a custodian (for example a family member, a lawyer, insurance company, or Workers' Compensation Board), even if it is with the consent of the patient, *the physician must notify the recipient of the purpose of the disclosure and the authority under which the disclosure was made.* The forms that you need to notify the recipient can be found at in the Forms and Letters templates (http://www.medicine.med.ualberta.ca/Library/Documents/staff/hia/lettersforms.pdf) document. If the patient has consented to the disclosure, use the form on page 17; if the custodian is disclosing without consent, use the form on page 18.

Handling a Request for Access to Information from the Patient or Authorized Individual

If the patient has a simple request for information, it should be dealt with immediately. For example, if the patient asks for copies of the last three letters sent to her family doctor, your office could simply photocopy them and give them to him or her – just be sure to ask the physician first and ask for identification if you do not know the patient by sight.

Likely the only time you would use the formal steps in a request for access to information is if there were a lot of information involved, or the custodian believes there might be reason to not disclose all of the information. If you receive a formal request for information, the steps can be found on page 29 of the

Health Information Act Guidelines and Practices Manual (http://www.health.gov.ab.ca/about/HIA_Guidelines-Practices-Manual.pdf). All of the required forms can be found in the Forms and Letters templates (http://www.medicine.med.ualberta.ca/Library/Documents/staff/hia/lettersforms.pdf) document. Here are a few key things to remember:

- All requests should be in writing with a signature.
- Date stamp any request for information with the date it was received because the physician must respond within 30 calendar days of this date.
- All requests should state what information is requested and why. Depending on the why the information is requested, they may not need all the information and the physician can advise them of this in case they want to modify their request.
- The request may be for copies of records or simply the opportunity to look through their record.
- Patients do not automatically have access to *everything* in their file. Physicians may decide to allow partial access to records or hold back certain information if they feel it may cause harm to the patient or others.
- A basic fee of $25 is usually charged to the patient for retrieving their records, plus additional fees for photocopying if the record is very large. The fees can be reduced or waived if the physician feels it is appropriate.
- Provide a name and contact information for the individual to approach if they have any questions or concerns.
- Whenever access to a portion of a file, or the whole file, is denied, the individual needs to be informed so that they may appeal to the Information and Privacy Officer.

Request for Correction or Amendment to Health Information

This is a similar process to the request for information, with one difference being the fact that no fees are involved. Once again, if the request is for a simple factual change (e.g. the birthdate recorded in their file is incorrect) the change should simply be made immediately. If there is any doubt, consult with the physician.

Like a request for access, a request for correction or amendment needs to be addressed within 30 days, unless an extension is required. Once the correction is made and the individual notified, everyone in the past year to whom the information was disclosed needs to be notified as well.

Questions?

Lisa Boehm
Dept of Medicine Information Coordinator
Phone: 407-3789
Fax: 407-3340
lboehm@ualberta.ca
www.medicine.med.ualberta.ca/Home/Staff/HIA/

Office of the Information and Privacy Commissioner
Phone: 422-6860
Fax: 422-5682
E-mail: generalinfo@oipc.ab.ca
www.oipc.ab.ca

University of Alberta
Information and Privacy Office
Phone: (780) 492-9419
Fax: (780) 492-6185
E-mail: foipp@ualberta.ca
www.ipo.ualberta.ca

HIA Help Desk
Alberta Health and Wellness
Phone: 427-8089
www.health.alberta.ca/about/health_legislation.html#HIA