Helping pharmacists and pharmacy technicians understand the *Health Information Act*

Privacy and confidentiality guidelines for pharmacy

August 2013 (updated 2018)

Alberta College of Pharmacy

Table of contents

Summary

The *Health Information Act* at a glance for custodians[1]

The *Health Information Act* (the HIA) sets out the rules for the collection, use and disclosure of health information by custodians.

The HIA definition of health information covers any information about an individual that is collected and recorded when a health service is provided.

The Act defines two types of health information:

- diagnostic, treatment, and care information, and
- registration information.

Technically, unrecorded infomration is not *health information*. Nevertheless, it is protected by the Act and may only be used or disclosed for the purpose for which it was provided.

The word *individual* is used here to include reference to persons who are authorized to exercise rights on behalf of an individual patient. Examples include a parent on behalf of a child, a guardian or trustee on behalf of a mentally incompetent patient, and a personal representative on behalf of a deceased individual.

Prime directive:
Collect, use, and disclose the least amount of information necessary and preserve the highest degree of patient anonymity possible to carry out the intended purpose.

General rules

- Only collect, use or disclose what is needed to do the job, no more.
- Collect directly from the individual whenever possible.
- Only provide information to those with a need to know.
- Provide anonymous information whenever possible.
- Safeguard the health information you hold.

Individuals' access to their own health information

- Individuals have a legal right to see or obtain copies of their personal health information without being asked why.
- Custodians have a duty to help individuals with their requests.
- In some circumstances, custodians can refuse access (e.g., when access may cause harm).
- Custodians have to respond to access requests within 30 days.

Corrections to health information

- Individuals have a right to ask for a correction or amendment to their information.
- Custodians can refuse to correct, for example, where the correction involves a

1 Adapted from *The Health Information Act At a Glance For Custodians*, produced by the Office of the Information and Privacy Commissioner of Alberta, 2012.

professional opinion.
- Individuals can ask the Information and Privacy Commissioner to review the custodian's decision or to append a statement of disagreement to their record.

Use of health information without consent

Custodians can use health information without consent for the following purposes:

- providing health services;
- determining eligibility for health services;
- conducting formal investigations including investigations, disciplinary proceedings, practice reviews, and inspections;
- conducting authorized research;
- providing health service provider education;
- complying with another piece of legislation; and
- managing internal operations such as planning and allocating resources, quality improvement, evaluation, and obtaining payment for services.

Disclosure of health information with consent

- Custodians can disclose an individual's health information with consent.
- Custodians must make sure they are disclosing information to the correct individual.
- Custodians must be reasonably sure the information is accurate.
- Keep a log of all disclosures made.
    - When disclosing a record containing individually identifying diagnostic, treatment or care information without consent, *including disclosure to another custodian*, the disclosing custodian must make a notation of
        - the recipient's name,
        - the date and purpose of the disclosure, and
        - a description of the information disclosed.
    - The disclosure notation may be in paper or electronic form, may be put on the individual's health or drug record or in a book or "disclosure log."
    - The notation must be kept for 10 years.
    - This requirement to log is not applicable when a custodian allows other custodians electronic access to individually identifying diagnostic, treatment and care information stored in a database, when the database automatically keeps an electronic log of a name or number that identifies the custodian to whom the information is disclosed, the date and time that the information is disclosed, and a description of the information that is disclosed (e.g., Netcare).

Disclosure of health information without consent

Custodians can disclose *without consent* to

- another custodian or police to prevent fraud or detect abuse of health services;
- another custodian or successor of a custodian;
- continuing treatment and care providers;
- family members in certain circumstances;
- individuals or authorized representatives of individuals;
- persons acting in the best interests of an incompetent individual;
- health professional bodies, auditors, and quality assurance committees;
- researchers subject to ethics review;
- entities authorized to obtain information or disclosures required by other legislation, e.g., courts and subpoenas;
- police when investigating a life threatening injury to the individual; and
- any person to avert or minimize an imminent danger.

1. Who sets the privacy rules for pharmacy professionals?

The *Health Information Act* (Alberta) (HIA)

Since 2001, registrants of the Alberta College of Pharmacy (you) and licensed pharmacies have been governed by the *Health Information Act* (Alberta) or HIA. This privacy legislation sets out the specific rules under which pharmacy professionals and other custodians under the Act collect, use, disclose, and protect health information in their custody and control.

In general, the HIA outlines specific practices and standards for health information privacy that apply internationally recognized privacy principles to personal health information in Alberta.

Other privacy legislation

Other health professionals or organizations that you may deal with may be operating under up to four other private and public sector privacy laws. For instance, an insurance company under the *Personal Information Protection Act* (Alberta) would likely require a valid consent from the patient before they can disclose information to you, even though you might be in compliance with the HIA in collecting the information without consent.

Professional ethics and the HIA

The pharmacy profession has a long history of safeguarding the confidentiality of personal health information as a vital component of their professional relationship with patients. The key concepts relating to patient privacy in the Alberta College of Pharmacy Code of Ethics closely mirror the key principles of privacy legislation.
The section on confidentiality provides high-level direction on major aspects of privacy.

Alberta College of Pharmacy

Code of Ethics

Principle IV: Respect each patient's right to confidentiality

To uphold this principle, I

- Inform each patient about the use that will be made of the patient's personal information, unless otherwise authorized by law.
- Disclose a patient's personal information only pursuant to the patient's consent or for the purpose of providing care to the patient, unless otherwise authorized by law.
- Inform the patient to whom and for what purpose the patient's personal information will be disclosed, unless otherwise authorized by law.
- Use information obtained in the course of professional practice only for the purposes for which it was obtained, unless otherwise authorized by law.
- Seek only information that is necessary to make informed decisions about the patient's health and the treatment alternatives that align with the patient's treatment goals, unless otherwise authorized by law.
- Protect each patient's privacy during any consultation.

Sections in the *Pharmacy and Drug Act*, *Standards for the Operation of Licensed Pharmacies* and *Standards of Practice for Pharmacists and Pharmacy Technicians* also provide guidance.

2. Key concepts and principles

Custodian vs. affiliate

QuickPoint:
Each registrant of the Alberta College of Pharmacy is a custodian under the HIA, except when they are an employee/agent or affiliate of another custodian (e.g., a staff pharmacist at a community pharmacy or AHS is considered an affiliate).

The HIA applies to health information generated by you when providing health services to patients. Pharmacists and pharmacy technicians are considered custodians under the legislation when they provide these services, even if the services are on behalf of a non-health care employer who may be governed by other privacy legislation. In such circumstances, you are directly and individually responsible as a custodian for ensuring compliance with the HIA for the health information in your care.

However, if you provide services on behalf of another designated custodian such as a community pharmacy licensee, Alberta Health Services, a nursing home, or another health professional, you are considered an affiliate of the custodian for which you provide services. That means that the custodian for which you provide services is responsible for your compliance with HIA rules and standards.

For a complete list of the healthcare professionals designated as custodians under the HIA, see the definition of custodian in Section 9: Definitions.

Privacy vs. confidentiality

QuickPoint:
Maintaining privacy means more than just safeguarding confidentiality—it is an ongoing program that involves accountability, control of information flow, right of access procedures, and security measures.

Information privacy has a much broader meaning than *confidentiality* (safeguarding information from unauthorized access). Privacy has been defined, generally, as the "right to be left alone" or to keep certain aspects of your life removed from public view. Living and working in a modern society, however, requires everyone to share information about themselves with people and organizations providing services to them.

In practical terms, then, information privacy is based on principles and measures aimed at giving individuals *control* over how others—and particularly health professionals—create, share, protect, and manage their personal health information.

To comply with current privacy standards, you need to go beyond just protecting the confidentiality of personal information you hold; you need to develop and participate in an ongoing privacy program that addresses

- accountability,
- information flow,
- right of access, and
- security.

Why is privacy so important to pharmacy professionals?

QuickPoint:
It's more than just compliance with a legal obligation to avoid sanctions—good privacy practices prevent harm to patients and directly support an essential component of successful pharmacy practice: patient and public trust.

Quality of care

A breach of patient confidentiality can result in significant harm to an individual, including long-term financial implications, compromised personal or professional reputation and identity theft. If patients can't trust pharmacy professionals with their most sensitive and personal health issues, they won't feel they can be open and frank with them—and that means health providers won't have the crucial information they need to provide an appropriate level of care.

You need to be aware of how technologies (e.g., Netcare, electronic medical records) can pose a risk of improper or unauthorized collection, use, loss, destruction or disclosure of personal health information.

Legislative and professional compliance

Compliance with laws is mandatory, and privacy laws stipulate sanctions for non-compliance. If you fail to comply with the legislation, an investigation by the Information and Privacy Commissioner of Alberta may result in a review, investigation or inquiry. Poor privacy practices can result in unprofessional conduct proceedings or other consequences. Sanctions for unprofessional conduct include reprimands, fines, imposing conditions on licences, and suspending or cancelling registration.

What is health information?

QuickPoint:
Health information links an identifiable individual with information about

- their physical or mental health, including drugs prescribed;
- the health service provider; and
- their contact and billing information.

The HIA operates with a very comprehensive definition of health information that covers any information about an individual that is collected and recorded when a health service

is provided.

The Act defines two types of health information:

1. Diagnostic, treatment, and care information—this includes information about
    - the physical and mental health of an individual;
    - the treatment they are receiving or have received, including information about health services providers involved in their care;
    - organ/tissue donations;
    - drugs prescribed;
    - health care aids; or
    - health care benefits.
2. Registration information—this includes
    - demographic information (name, ID, personal health number (PHN), date of birth, gender);
    - location, residency, and how to contact;
    - health service eligibility; and
    - billing.

Health information is considered "non-identifying" if the individual cannot be readily identified from the information. By and large, the HIA has few rules for the collection, use, or disclosure of non-identifying health information, so long as the individual identity remains hidden.

Roles and policies

QuickPoint:
Each pharmacy professional or practice must designate a Privacy Officer responsible for implementing the custodian's privacy program, backed up by privacy policies and procedures.

Privacy accountability means that your privacy program responsibilities and policies are clear and transparent to the general public. Each pharmacy professional or practice must identify a "responsible affiliate" who will be their Privacy Officer (HIA s.62). This person is named on all privacy notifications and will process right of access requests. In addition, the professional or practice must develop and follow specific policies and procedures for implementing the custodian's HIA privacy program (HIA s.63).

Key concepts FAQs

Is the head office of my pharmacy chain the custodian of the health information I collect and handle in my practice?
No. The pharmacy licensee is the custodian of this health information and other pharmacy professionals or administrators who work for this person are affiliates. If the corporation provides information management, processing or storage services for the pharmacy practice, it would be providing services as an affiliate as well, and specifically as an information manager, which has a distinct status under HIA s.66.

What if I am employed as a pharmacy professional by another organization or company, such as a hospital or a service within Health Canada?

If the company or organization is another custodian, such as Alberta Health Services, you are an affiliate of that custodian, and not a custodian yourself. If, however, your employer is not a custodian under the HIA, such as a pharmacy service for First Nation communities operated by Health Canada, you would be considered a custodian in your own right.

If information drawn from a health record doesn't contain the name of the patient, is it still health information under the HIA?

If the identity of the subject of the health information cannot reasonably be drawn from the health records, it is considered non-identifying health information. That doesn't just mean that the name of the subject has been removed—if the information contains the personal health number (PHN), address, or phone number of the individual, for instance, it is considered identifying health information because the identity of the subject can be inferred using other sources.

3. Sharing health information under the HIA: an overview

QuickPoint:
The HIA is designed to enable, not restrict, the flow of health information among health providers within the circle of care of a particular patient. Disclosure outside of this circle is more strictly controlled.

Figure 1 illustrates the flow of health information both within and outside of the circle of care.

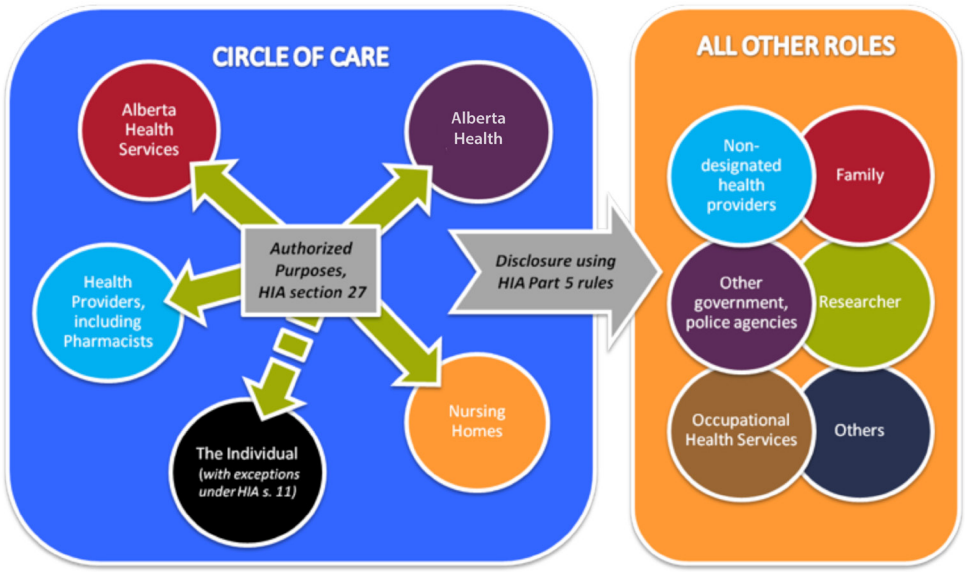

Figure 1: Sharing health information within and outside of the circle of care

Simply put, you can, without patient consent, share health information about patients with other custodians within the circle of care so long as it is connected to specific authorized purposes related to administration and delivery of health care for the patient.

The guiding principle for exchanging information within the circle of care for these purposes is that the least amount of health information with the highest degree of anonymity should be shared among custodians.

For disclosure to non-custodians and others who are not part of the circle of care, and/or for purposes that are not authorized, Part 5 of the HIA outlines specific circumstances where use and disclosure may be allowed.

Individual patients, of course, regularly receive from and disclose their own health information to you as part of their health services and can exercise their right of access; you, however, can withhold from individual patients some of their own health information under exceptional circumstances outlined in the HIA Part 2.

The insert below explains the authorized purposes for collecting, using and disclosing health information when operating within the circle of care.

Authorized purposes for collecting, using, and disclosing health information without consent within the circle of care (HIA s.27)

- providing health services;
- verifying eligibility to receive a health service;
- investigations, practice reviews, or inspections of a health professional;
- research that has been approved by a designated research ethics board;
- to facilitate health service provider education;
- for a purpose authorized by statute; or
- to support internal management, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, processing payments, or human resource management.

4. Collecting and using health information

Limiting how much health information is collected and used

QuickPoint:
Pharmacy professionals must only collect and use the least amount of health information required for the specific authorized health care purposes listed in the HIA. Patient consent is neither required nor sufficient.

Properly managing and protecting health information starts with ensuring that you collect the right information about a patient for the right purposes. Once you have health information about the patient in your custody and control, you then have to make sure that you and your employees use the information in the same way.

You may only collect and use health information about individuals for one of the authorized purposes listed under HIA s.27 (see authorized purposes). Consent of the individual is neither required nor adequate for you to *collect* health information in compliance with the HIA.

Consent is required, in some cases, when you *disclose* health information to non-custodians, and/or for purposes that are not authorized under HIA s.27.

You need to limit the amount and type of information you collect and use to the least amount of health information essential to carry out the authorized purpose, with the highest degree of anonymity possible. For instance, you should collect information like email addresses only if it is needed for purposes such as medication notifications, but not for sending out notifications to customers about special sales or events.

By the same token, once it is collected, pharmacy affiliates are not free to use health information for any purpose. Employees of a pharmacy processing prescriptions for patients, for instance, should only be accessing the records of those patients to whom they are delivering services; access to records of other patients must be justified by one of the authorized purposes.

For the most part, you will collect and use health information to provide health services. The details about what information is required as part of best pharmacy practices is documented in ACP standards of practice.

Indirect collection

QuickPoint:
Pharmacy professionals can collect health information from someone other than the patient for a variety of practical purposes and circumstances.

As a general rule, you should try to collect personal information directly from the patient. However, there are many instances where you collect health information indirectly from sources other than the patient, including confirming a prescription with a health provider or getting information from the patient's record in the provincial *Pharmaceutical Information Network* system.

The HIA recognizes a number of circumstances where indirect collection is allowed. This includes the following

- The collection is authorized by the patient in some way.
- Collection from an authorized representative (not just a family member) of the patient.
- When, on reasonable grounds, you believe that collecting information from the patient would prejudice the interests of the patient, the purpose for collecting the information, or the safety of anyone else, or would result in inaccurate information being collected (e.g., a patient can't remember the names of other medications they are taking).
- Where direct collection is not practical, such as when the patient is sick or incapacitated, or because of urgency.
- When the information is from a public source.
- To determine or verify eligibility to receive a benefit, product or health service;
- To fulfill a request from the Public Guardian or Public Trustee.
- To complete a genetic/family history as part of a health service to the patient.
- To facilitate an authorized research project.
- When another custodian is disclosing the information to the pharmacy professional under any of the conditions listed in HIA Part 5 (see Section 5, Disclosing health information) (e.g., with their consent, from another custodian for health purposes, to detect fraud).

Note as well that there may be times when you need to collect health information from another source without the patient's knowledge or consent in order to, for instance, investigate a case of fraud or abuse of health services. If the information was given implicitly or explicitly in confidence, the identity of the source can be protected, so long as it reasonable to do so under the circumstances (e.g., the source may be exposed to undue harm).

Notification

QuickPoint:
Every patient should be able to know what information about them is being collected and used by a pharmacy professional, and why.

When collecting information directly from patients, it is important that you notify patients of the specific purposes and authority for the collection. The notice must be given up front in a clear, understandable form and provide the name of the official in the practice who can answer questions about the collection. The notification can be done through brochures, posters, or one-on-one consultations (see Appendix 1: Sample notification for collection of health information).

Collection and use summary

Figure 2 is a summary of the processes and decisions you need to complete as part of your collection and use of health information. The duration and complexity of the process flow will vary greatly depending on the circumstances.

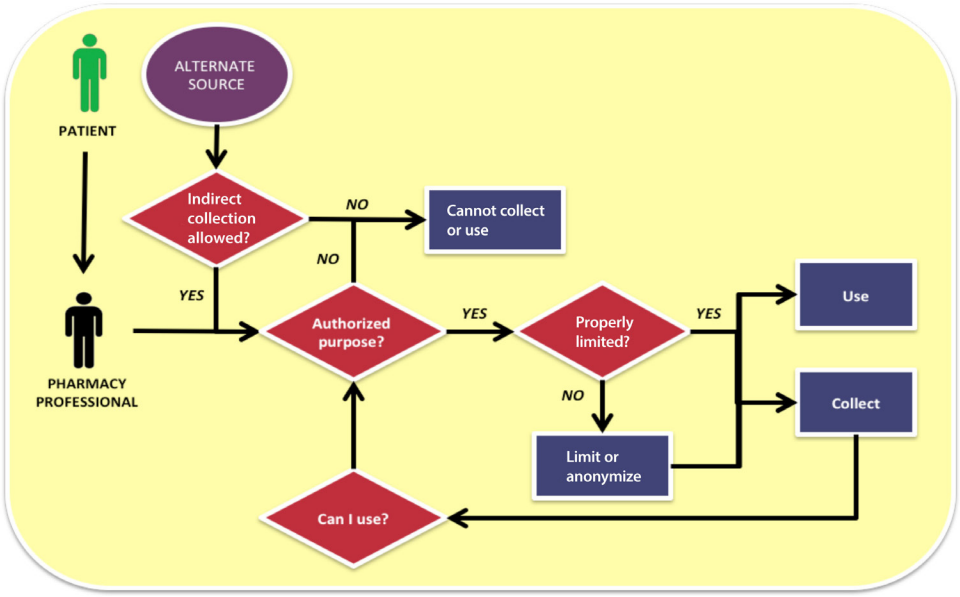

Figure 2: Collection and use process flow

Collection and use FAQs

Can I collect health information about a patient from family members to fill a prescription?

This is an indirect collection and is allowable if the patient is incapacitated and not reasonably able to present and fill their prescriptions themselves, or if the family member is an authorized representative (e.g., parent of a minor). Otherwise, you will need some reasonable indication that the patient has authorized the family member to provide you with their health information.

A good practice is to get from the patient the first time they are able to be present the names of others who might provide or receive information on their behalf. Otherwise, the fact that the patient is covered by the family member's health insurance may be a good indicator that the person is acting on the patient's behalf. If there is any doubt about the veracity of the information or status of the person providing the information, contact the patient directly before completing the collection.

If my patient asked me to collect health information directly from his or her physician that I need to confirm a diagnosis, could the physician refuse to provide it?

As the patient is expecting you to deliver a health service for him or her, you are collecting the information for an authorized purpose (provision of health services, HIA s.27(1)). Under College of Physicians & Surgeons of Alberta's (CPSA) standards of practice and code of ethics, physicians are required to collaborate with other health professions in providing health services, making refusal a rare occurrence. However, the physician does have the right to refuse to provide information in their custody and control, even if it is allowed under HIA disclosure rules. In this case, the patient would have to obtain the information themselves from the physician to give it to you.

Why is the patient's personal health number required as part of patient demographics?

The personal health number (PHN) is the unique identifier that is used by other health professionals to identify the patient. In addition to allowing you to identify the patient accurately, collection and use of the PHN will allow for sharing of information in the Alberta electronic health record and support health system management, planning and resource allocation in Alberta.

- HIA s.21 specifically authorizes you, as custodian, to require collection of the PHN from patients when you provide services.
- HIA Regulation s.7.1 requires you to provide a patient's PHN to Alberta Health as part of a dispensing record.

In all cases, you need to notify patients of your authority to require their PHN.

What if the patient refuses to provide their personal health number?

If, after proper notification, an individual is still apprehensive about providing their PHN, explain to them

- the importance of this number in uniquely identifying their record within the pharmacy and the health system;
- how important it is for you, as a member of their health team, to have this number to ensure that their drug therapy information is entered only on their record;
- the importance of having their drug therapy information accessible to other healthcare professionals, through their EHR, if they become ill and cannot speak (e.g., stroke or unconscious from an auto accident); and
- that collecting their PHN is one more step you are taking to keep them safe.

If the individual refuses to provide their PHN, despite your explanation, DO NOT refuse professional services unless not having the PHN prevents you from having information that you need to provide the health service. Proceed to provide the services as you normally would, and do your best to ensure that their drug therapy information is entered on the correct record.

Can pharmacy professionals require that patients provide them with their driver's licence in order to verify their identity?

Yes, you may ask to see identification such as a driver's licence, but should not record as it would not be a collection under the HIA. (See summary of the OIPC ruling on this issue.)

5. Disclosing health information

Limiting disclosure of health information to authorized purposes

QuickPoint:
Pharmacy professionals can disclose to other custodians within the circle of care the least amount of health information required for the specific authorized health care purposes listed in the HIA. Patient consent is not required.

As with collection and use of health information, you need to limit the amount and type of information you disclose to the least amount of health information essential to carry out the purpose, with the highest degree of anonymity possible. In addition, if a patient explicitly makes a request to limit disclosure of their health information to, for instance, certain health providers, you must closely consider and be prepared to accommodate this request if it is reasonable and practical.

Disclosure to the individual who is the subject of the information is dealt with in Section 6: Giving individuals access to their own information.

Disclosure for other purposes

QuickPoint:
The HIA lists over 25 specific circumstances where a pharmacy professional can disclose health information to others and for purposes outside of the circle of care. Patient consent is not required.

Part 5 of the HIA lists a significant number of circumstances in which pharmacy professionals would be able to disclose health information to non-custodians for other purposes, without the consent of the patient. These are enabling provisions, *not* requirements to disclose. You are allowed, but not obligated, to disclose patient information without consent under the circumstances presented.

Allowances for disclosure of health information without consent outside of the circle of care (HIA s.35-45)

- To the government of Canada or another province or territory, for health system management, if:
  - The patient is a resident of that region; or
  - That government is paying for the health service;
- To the person providing continuing care of the patient, including family, friends or other non-medical support;
- To family members or close personal friends:
  - If it is limited to presence, location, condition, diagnosis, progress, and prognosis on that day;
  - To contact them if the patient is incapacitated or deceased; or
  - To provide information about circumstances or health service provided surrounding the patient's death; and
  - The disclosure is not against the expressed request of patient;
- To a correctional program officer, for health service or continuing care purposes;
- To a person conducting an audit, if the person agrees in writing:
  - To destroy the information as soon as the audit is completed;
  - Not to disclose the information to anyone other than to report unlawful or improper conduct of a health service provider;
- To a quality assurance committee under *Alberta Evidence Act*, Section 9;
- As part of court or quasi-judicial proceeding to which the pharmacist is party;
- To comply with a court order, warrant or subpoena valid within the jurisdiction (mandatory);
- To another custodian, as part of an investigation of fraud, abuse of health services, or to prevent commission of a statutory offence;
- To an officer of the Legislature, for the performance of their duties;
- To avert imminent danger to the health or safety of anyone;
- If it is in the best interests of an individual who lacks capacity to consent;
- To a descendent of a deceased individual if necessary for the health of the descendant;
- As allowed or required by other laws, in spite of HIA provisions;
- To a custodian who is the successor of a custodian;
- To obtain or process payment for health services;
- To the College of Physicians & Surgeons of Alberta in compliance with the Triplicate Prescription Program;
- To a health professional body, as part of a complaint or investigation;
- For the purpose of assessment and storage at a public body archives; or
- For registration information only, to collect or process a debt or fine owing, or to an ambulance attendant or operator.

Disclosure to law enforcement

QuickPoint:
You may disclose without consent a limited amount of patient health information in your custody to the police to prevent or limit fraud or to protect public safety.

You may be asked or may feel that it is necessary to report to the police or other law enforcement agencies contact information or other health information about a patient. This disclosure to the police is allowable under specific circumstances.

You may disclose health information to a police service or to the Alberta Ministry of Justice without the individual's consent if you reasonably believe that the information disclosed relates to the possible commission of an offence under a statute of Alberta or Canada and will either

- detect, limit or prevent fraudulent use or abuse of the health system (HIA s.37.1), or
- protect the health or safety of an individual (HIA s.37.3).

The disclosure must be limited to the following information, as required:

- the individual's name, birth date, and personal health number;
- the nature of any injury or illness of the individual;
- the date on which a health service was sought or received;
- the locations where the health service was sought or received;
- the name of any drug provided or prescribed to the individual, and the date the drug was provided or prescribed;
- whether any samples of bodily substances were taken from the individual, or
- information about the health provider who provided the service.

Log the disclosure and keep on the individual's record for at least 10 years.

Disclosure for health system or Alberta EHR purposes

QuickPoint:
Alberta Health or another custodian could request and sometimes require a pharmacy professional to disclose specific health information to them for health system planning, surveillance, or management purposes, or for submission to the Alberta EHR .

Alberta Health collects information about the operation and functioning of the health system in Alberta. Alberta Health will therefore request that custodians submit to them certain health information of their patients as part of this health system assessment, planning, surveillance or management process. The HIA makes it mandatory that you disclose health information to Alberta Health upon request if it relates to health service directly paid for or supported by the government. The disclosure does not require patient consent but a Privacy Impact Assessment must be completed before the disclosure can be made. A similar request can be made by another custodian for health system planning within their area, but in such cases you could refuse based on individual and public safety concerns.

Pharmacy services are a key factor in health system planning and a priority service for inclusion in the Alberta Electronic Health Record. The HIA lists the specific data elements that Alberta Health may request from you for submission to the Alberta Netcare Pharmaceutical Information System (PIN):

- patient name, gender, date of birth, and personal health number;
- drug identifier;
- prescription, dosage, and dispensing details; or
- prescriber and pharmacy professional identifiers.

Research disclosure

QuickPoint:
Researchers must have their proposal approved by a Research Ethics Board before a pharmacy professional can allow them access to health information of their patients or the patients of other health providers.

You may wish to use or receive a request to disclose some of your health information for research. The research proposal must have approval of one of the Research Ethics Board designated in the HIA. You, as custodian, then consider the proposal and have the option of refusing the disclosure. If and when you do approve, disclosure for research purposes must follow any conditions set by the Research Ethics Board. The researcher must also sign an agreement with you as outlined in the HIA that requires the researcher to meet specific security and confidentiality practices and standards.

Logging disclosures

QuickPoint:
All disclosures must be properly documented or "logged" in some form, either manually or electronically, including the date, purpose, recipient, and description of the information disclosed.

If a custodian discloses a record (within or outside the circle of care) that contains individually identifying diagnostic, treatment and care information, without consent, the custodian must log that disclosure. The log must contain

- the name of person to whom information was disclosed;
- the date and purpose of the disclosure; and
- a description of the information disclosed.

This information may be kept as a separate disclosure log (paper-based or electronic) or may simply be any documentation kept in a record that provides the same data whenever it is subsequently requested.

The requirement to make a note does not apply to custodians that permit other custodian electronic access when the electronic system automatically keeps an electronic log of the information listed.

The notation or electronic log must be retained for at least 10 years (HIA S. 41(2)).

In addition, if you are disclosing to anyone other than another custodian, the police, or to the patient, you must inform the recipient of the purpose of the disclosure and the authority under the HIA you are using to allow the disclosure.

Disclosure logs are critical when information is lost, manipulated in an unauthorized manner, when a recipient needs to be notified of a correction, or in the event of a privacy breach. Disclosure logs are needed to support accountability in the management of individually identifying health information.

Consent

QuickPoint:
A pharmacy professional can obtain the consent of the individual to disclose health information, but it must be written, explicit, and include all the prescribed elements.

You do not need the consent of the individual to collect, use or disclose their health information for authorized purposes or in accordance with disclosure allowances. However, there may be infrequent situations where it may be necessary to use or disclose health information for reasons and in circumstances that do not meet these criteria. In such cases, you must obtain explicit and written consent of the patient or other individuals who are the subject of the health information.

Where consent is required, it must be part of a process where the patient is fully informed and not subject to unreasonable pressure to decide one way or the other. Be sure to get the consent *before* you disclose information—consent collected after the fact is not valid.

A consent under the HIA must contain the following elements:

- an authorization from the individual or authorized representative;
- the purpose for collection, use, or disclosure;
- the users or recipients of the personal information;
- an acknowledgement that the individual providing the consent understands the risks of consenting or not consenting;
- the effective date and, if any, the expiry date of the consent; and
- a statement that the consent may be revoked by the individual at any time.

Only the patient or individual or one of their authorized representatives can sign the consent.

Consents are by nature voluntary, so not only can the patient and individual refuse to consent, they can withdraw a consent they've already given. If this occurs, you are not required to destroy the information since it might be needed for evidentiary purposes, but must cease to collect, use, and disclose it for business purposes. You should always, within reason, seek alternatives where you can still provide health services without the personal information. As always, a minimum quality of care should never be compromised.

Appendix 2 is a model form for obtaining a valid consent under the HIA.

Disclosure summary

The decision flow diagram below (Figure 3) summarizes the considerations you might need to make to respond to a request from outside your practice or organization for the health information you hold as a custodian. Note that this does not cover right of access requests from individuals who are the subjects of the health information.

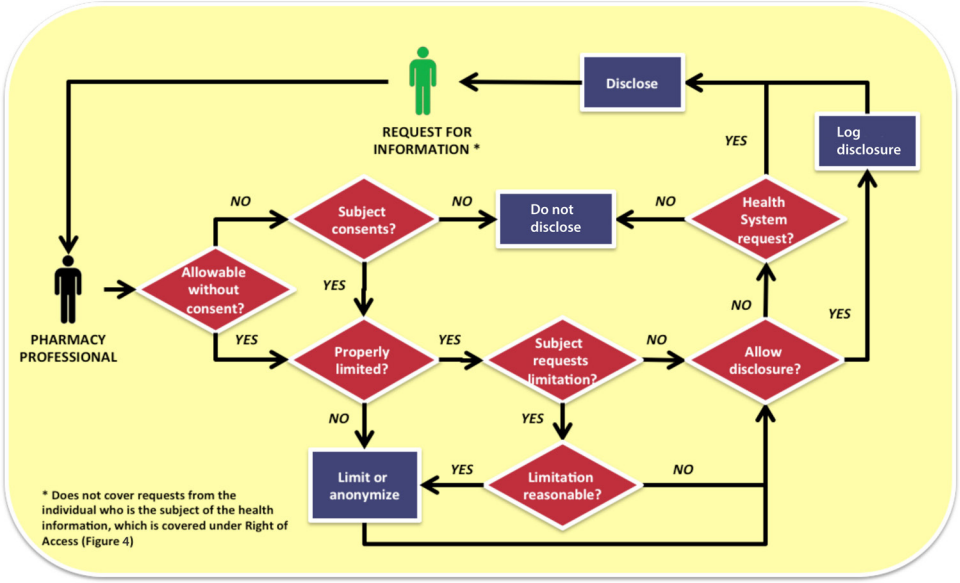

Figure 3: Disclosure process flow

Disclosure FAQs

When do I have to keep a record of disclosure?
Whenever there is a disclosure of health information within or outside the circle of care, the pharmacy professional responsible must ensure that the following information is logged about the transaction and that it is retained for at least 10 years:

- name of person to whom information disclosed;
- date and purpose; and
- description of information disclosed.

This information may be kept as a separate disclosure log (paper-based or electronic) or may simply be any documentation kept in a record that provides the same data whenever it is subsequently requested.

Note: You do not have to log the disclosure if you upload the information onto Netcare. The requirement to make a note does not apply to custodians that permit other custodians electronic access when the electronic system (e.g., Netcare) automatically keeps an electronic log of the information listed.

Can I disclose information to the police if I suspect a forged prescription?
You may disclose health information to a police service without the individual's

consent if you reasonably believe that the information disclosed relates to the possible commission of an offence under a statute of Alberta or Canada and will either

- detect, limit or prevent fraudulent use or abuse of the health system (HIA s.37.1), or
- protect the health or safety of an individual (HIA s.37.3).

In this case, both of these criteria could reasonably apply—uncontrolled distribution drugs obtained through fraud could certainly present a danger to public health and safety. The disclosure must be limited to the following information, any of which may be required by police to complete the investigation:

- the individual's name, birth date, and personal health number;
- the nature of any injury or illness of the individual;
- the date on which a health service was sought or received;
- the location where the health service was sought or received;
- the name of any drug provided or prescribed to the individual, and the date the drug was provided or prescribed;
- whether any samples of bodily substances were taken from the individual, or
- information about the health provider who provided the service.

Document the disclosure on the individual's record and to keep it for at least 10 years.

Can I release patient information to a home care nurse?

Pharmacists and pharmacy technicians are allowed to disclose a patient's prescription information to a home care nurse without the consent of the patient (s.35 of HIA). There are two provisions that may apply:

- The nurse is likely a custodian under the HIA, even if they are not employed by another custodian. You may disclose to another custodian without consent for any authorized purposes (s.27).
- You may disclose without consent to a person, such as the home care nurse, who is responsible for providing continuing treatment and care to the individual.

Remember to document the disclosure on the patient's record and to keep it for at least 10 years.

How should I handle the disclosure of health information to family members, e.g., prescription receipts, releasing a prescription to a family member?

The HIA allows you to disclose health information without patient consent to family members or close personal friends:

- if it is limited to presence, location, condition , diagnosis, progress, and prognosis on that day;
- to contact them if the patient is incapacitated or deceased; or
- to provide information about circumstances or health services provided surrounding the patient's death; and
- the disclosure is not against the expressed request of patient.

Release of prescription receipts and prescription information, for instance, do not match these provisions.

You may also disclose without consent to individuals, including family or friends, who are providing continuing care or treatment for the patient, including picking up prescriptions for them.

This would not cover providing a printout of prescription receipts for tax purposes, however, since this is not part of continuing treatment and care. In cases such as tax

receipts and other non-continuing care matters, the person requesting the information must be an authorized representative of the patient, which includes

- guardian of a minor who is not competent to understand their rights (careful with minors aged 14-18!);
- Personal representative for the administration of a deceased individual's estate, for estate purposes;
- Guardian or trustee under the *Adult Guardianship and Trusteeship Act*;
- Agent under the *Personal Directives Act*;
- Attorney under power of attorney;
- Nearest relative of a formal patient under the *Mental Health Act*;
- Person with written authorization from the individual to act on the individual's behalf.

Be sure to verify the status of the recipient. If they are not an authorized representative, you will need the written consent of the patient before you disclose the information.

As always, document the disclosure unless it was to an authorized representative, and keep it for at least 10 years.

What if I have verbal consent from a patient to disclose health information to someone else?

Verbal consent, or other alternatives such as implied or opt-out consent, is not valid under the HIA. To be valid, the consent must be written and must specify

- what information may be disclosed, to whom, and for what purpose(s);
- the date the consent becomes effective;
- when the consent expires (if at all);
- an acknowledgement that the individual consenting understands the risks of consenting or not consenting; and
- that the consent can be revoked at any time.

A sample valid consent form can be found as Appendix 2.

Once again, you need to document each disclosure (the consent itself may not be enough since you may disclose several times under one consent). All of this documentation, including the consent, must be kept for at least 10 years.

Can I disclose information about patients other than my own in Netcare or disclose health information that other health providers have entered and that I have access to?

You should only disclose information relating to patients for whom you are providing services. This could include information you needed to access in Netcare about your patient that other providers have entered into the system. At the same time, you shouldn't be disclosing information in Netcare about anyone other your own patients, even if it is for authorized purposes, mainly because you wouldn't be able to judge accurately whether any of the disclosure allowances or authorized purposes can be applied accurately.

What if the patient explicitly requests that some or all of their health information not be disclosed to another health provider or another individual under any circumstances?

You are required to consider any expressed wishes of the patient when deciding whether and what to disclose, even as part of the Alberta EHR, together with any factors that you think are important. For instance, a patient might ask to ensure that her ex-husband,

who is a physician, does not know that she is taking medications and therefore does not want you to submit her information to PIN (even though the physician would be prohibited from accessing the file). If the physician is still practising, and considering the circumstances described by the patient, this might seem reasonable. In other circumstances, it may be your judgement that not disclosing health information to other health providers is too much of a risk to the safety of the patient or the ability of a healthcare professional to provide appropriate health services, including circumstances of a medical emergency. In the end, after due consideration, the decision to disclose is still yours to make in spite of the objections of the patients, and you should document this consideration process.

Because information in Netcare is automatically made available to authorized healthcare providers as required, requests by patients to withhold all or part of their health information from disclosure present a challenge. Alberta Netcare has developed procedures, criteria and scripts for masking information globally at the person level in their systems to fulfill these requests. Health providers may still "lift the mask" or can apply to rescind masking applied to records of their patients as required for specific reasons documented in the system.

If licence and location information about a pharmacy professional is health information, can I disclose this on my pharmacy's website?
Yes, you can and you must in compliance with s.23 of the Pharmacy and Drug Regulation.

Do I have to document *all* disclosures?
Examples of disclosure that must be documented

- Providing a filled prescription to a person other than the patient or the patient's agent;
- Giving a person, other than the patient, counselling information or instructions in writing for a prescription where the information is specific to that patient;
- Faxing a doctor or doctor's office to confirm prescription for a change, refill, etc.;
- Faxing a therapeutic monitoring profile to home care for the medication assistance program.

Examples of disclosure where documentation is not required

- Disclosing information about the patient directly to that patient or that patient's authorized representative;
- Using a patient's information within the pharmacy among affiliates, including your information manager;
- Disclosing non-identifying health information.
- Verbal disclosure of health information among custodians.

6. Giving individuals access to their own health information

The right of access

QuickPoint:
All individuals have a right of access to their own personal information—it can't be limited or waived except by legislation.

A fundamental principle of privacy legislation is that individuals have right of access to their own personal information kept by any organization, including their employer. Patients may request information contained in their health record for any reason, including for the purposes of a dispute with a pharmacy or pharmacy professional. It is important, therefore, that the access process be designed from the outset to be open, consistent, and compliant with the HIA.

Exceptions to the right of access

QuickPoint:
The HIA identifies a limited number of mandatory and discretionary exceptions to an individual's right of access. If these exceptions do not apply, the information must be released.

Only the individual the information is about has the right of access to the information. This doesn't include family members or others, unless the person is an authorized representative of the individual. The other specific situations where access may be given to people other than the subject of the information are covered in Section 5: Disclosing health information.

You *must* refuse to provide access to information when it is about another person, unless the other person consents to the access or when the information was provided by the person who is now requesting the information.

Exceptions to an individual's right of access to their own health information (HIA s.11)

Mandatory

- information is about another person, unless the applicant provided it;
- reveals procedures or results of a formal investigation of a pharmacy professional or other healthcare providers; or
- prohibited by another Act.

Discretionary

- likely to result in immediate or grave harm to patients or others, or threaten public safety;
- will reveal the identity of an information source if it was provided in confidence for reasonable purposes;
- reveals advice or deliberations of a health region or Alberta Health in consultation with the pharmacy professional; or
- prejudices the results of an audit or standardized test.

If a file or document contains information that is not to be released, you must "sever" or take out information so that the rest of the file or document can be released. For instance, if you or another pharmacy professional is under investigation, and information about the investigation relates to the patient who is requesting their information, you will need to withhold documents, sections, or even individual words that would reveal procedures or results of the investigation.

Request process for access to health information

QuickPoint:
Don't use the formal HIA right of access process if the information requested clearly doesn't require review to release. If it does, you must follow the formal 30-day process prescribed by the HIA, under the direction of the Privacy Officer.

You give patients information about themselves routinely as an integral part of their health services. Sometimes patients may even ask to access basic additional health information about themselves that you may have on file (e.g., previous prescriptions, contact information). All of these can be handled as informal, routine releases so long as there is clearly no information in the record that will need to be withheld and the information can be accessed easily.

In all other cases, where there appears to be third party information in the records requested or other exceptions to access may apply, the request should be treated more formally. Formal requests should be made in writing and forwarded to the Privacy Officer, who is responsible for this task in your practice.

The HIA requires that you respond to all right of access requests within 30 calendar days—if you don't, your response will by default be regarded as a refusal. Although there are provisions for extensions of time limits, these provisions are specific and include criteria that must be met by the custodian (e.g., the request is so voluminous that extended time is needed to facilitate request processing).

Steps for processing right of access requests

1. Verify that the requester or "applicant" is who they say they are or establish that the necessary authorization is in place.
2. Work with the applicant to clarify the scope and nature of the information requested if it is unclear.
3. Find and review thoroughly all information relevant to the applicant's request.
4. Document clearly any information you have severed along with the legislative exception that applies. This is important for two reasons:
    a. In your response to the applicant, you must inform them that information has been withheld or severed and why;
    b. Should the applicant ask for a review by the Office of the Information and Privacy Commissioner, you will be required to recreate your complete review process.
3. Along with the information requested and any severing documentation in your response, you must also instruct the individual on the avenues available to challenge the decision. Encourage the applicant to first bring their complaint or concern to your organizations' Privacy Officer. If this is unsuccessful, the applicant can make a formal complaint to the Information and Privacy Commissioner of Alberta.

You have a general duty to assist anyone requesting their own information and should be prepared to explain the meaning of any codes, abbreviations, or terminology in the records.

Individuals may either view the original record or request a copy. To preserve the integrity of the record and ensure that documents are not removed from the premises, you need to supervise an individual reviewing an original record.

Individuals should normally not be charged for access to their own personal information if the size and complexity of retrieval and review are minimal. However, specific maximum rates and fees, outlined in the HIA Regulation, may be charged for processing the request and for reproduction, transcription, or transmission of information, so long as the individual is notified before these costs are incurred. The individual must be given an estimate of the fee in advance and the final charge must represent actual costs incurred.

Use of the formal HIA right of access process should occur only rarely. Additional information and help is available from Office of the Information and Privacy Commissioner.

Requests to correct or amend health information

QuickPoint:
Correct or amend factual inaccuracies in a patient record; don't correct professional opinions or records created by others.

You have a duty under the legislation to collect, use, and disclose personal information that is as accurate and complete as reasonably possible. Individuals have a right to request correction of personal information held by a custodian.

As with requests for access, requests from individuals to correct or amend basic health registration information about themselves (e.g., change of name or address) are handled as a routine release of information.

Formal requests to correct or amend personal health information must be in writing and can only be submitted by the individual who is the subject of the information or their authorized representative. All formal requests must be accompanied by appropriate documentation to support the request and must be processed within 30 days of the receipt of the request.

Any information that is factually correct should not be changed or amended. In addition, you should not amend either your own or your colleagues' professional opinions, or records (such as a prescription) that were created by another health professional. **If amendments are to be made, do not delete the original information, but simply cross it out.**

If the custodian refuses to make the correction or amendment, the custodian must, within the 30-day period (or during the extended period), tell the applicant of the refusal to correct or amend and give the reasons for refusing.

If a correction or amendment is refused, the applicant can either request a review by the Information and Privacy Commissioner or submit a statement of disagreement that must be attached to the relevant records. Third parties who have received the information up to a year previously must be given a copy of the statement of disagreement by the custodian.

Right of access summary

The diagram below (Figure 4) summarizes the decisions and steps needed to properly process a right of access request under the HIA.

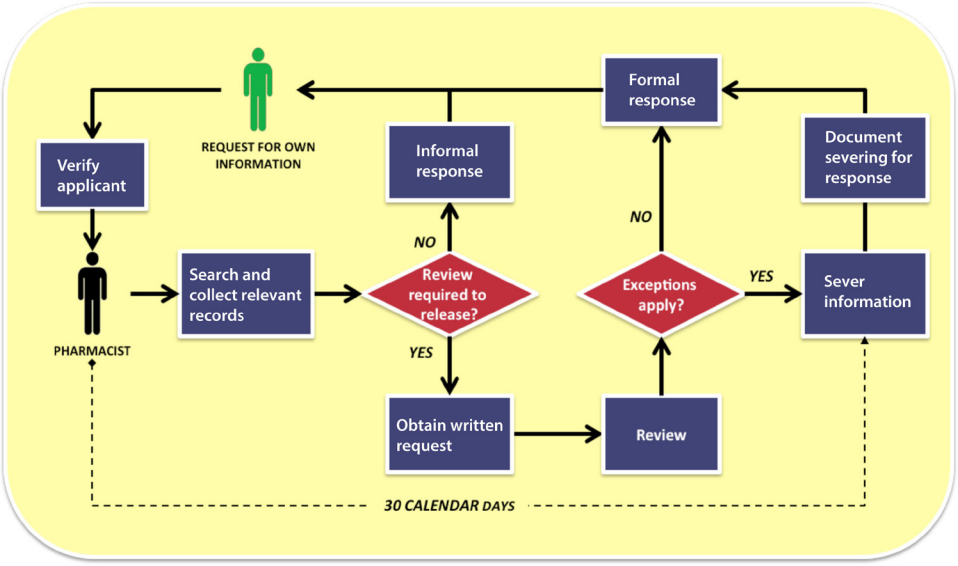

Figure 4: Right of access request process flow

Right of access FAQs

Do I need to go through the formal right of access request process under the HIA every time a patient or someone else requests their health information?

No. In fact, a formal right of access request should be a relatively rare occurrence. The great majority of these requests can be handled as informal, routine releases so long as there is clearly no information in the record that will need to be withheld and the information can be accessed easily. In other cases, where there appears to be third party information in the records requested or other exceptions to access may apply, the request should be treated more formally. Formal requests should be made in writing and forwarded to the Privacy Officer, who is responsible for this task in your practice. They will need to respond to the applicant within 30 calendar days.

If an individual to whom I have not provided health services makes a right of access request or request for correction for information in Netcare that I have access to, do I need to process this request?

No. As with questions about disclosure of this kind of information, you should only process right of access requests for information relating to patients for whom you have provided services. This could include information you needed to access in Netcare about your patient that other providers have entered into the system. At the same time, you shouldn't be reviewing information in Netcare about anyone other than your patients and therefore shouldn't be making right of access decisions about this information.

For requests for correction or amendment of information in Netcare, under HIA s.13(6) you can refuse to correct information about the individual that was entered into Netcare by another health provider, even if the individual is your patient.

7. Securing health information

The need for information security

QuickPoint:
Because health information is so sensitive, the HIA requires pharmacy professionals to institute and maintain a comprehensive information security program for protecting the confidentiality and integrity of health information in their custody and control.

Personal health information ranks very high in sensitivity and can result in serious repercussions to the individual if their information is breached. Therefore, the HIA sets out extensive criteria and standards for custodians to protect health information in their custody and control, including the following administrative, technical, and physical safeguards:

- identify and mitigate threats and risks of unauthorized use, disclosure, modification, or loss of health information, including electronic formats;
- submit a Privacy Impact Assessment for proposed new systems, policies, or practices affecting health information management;
- protect health information stored or disclosed outside of Alberta;
- have secure information disposal practices;
- develop information security policies; and
- designate an information security officer.

Below are some practical tips for securing health information in your custody and control.

Physical and technical security tips

- When taking or discussing patient orders, ensure that conversations or health information on screens or documents cannot be overheard or viewed by others.
- Designate clearly marked patient service areas and segregate these areas with physical barriers.
- Do not leave records containing personal information unattended in patient service areas and other public places.
- Adopt a clean work area rule. Clear off work areas at the end of each day (or when leaving your work area for an extended period of time) and lock records containing personal information in desks, cabinets, safes, or rooms.
- Log off systems that contain personal information when you are away from your work area.
- Ensure that files containing personal information are protected by the use of passwords. Change passwords regularly and do not disclose or record them in areas accessible by others.
- Ensure that electronic records on your hard drive are backed-up at regular intervals.
- Ensure that records containing personal information are not saved on an unprotected shared drive.
- Mail personal information using securely sealed double envelopes, stamping the inside envelope CONFIDENTIAL and identifying the intended recipient.
- Erase boards and remove documents, drawings, flip charts and other records

containing personal information from meeting areas.
- Do not post or make personal information viewable by the general public or by employees.
- Lock file rooms and computer rooms.
- Restrict casual visitors to designated areas.
- Ensure protective measures are taken when records with personal information are in transit.
- Take all necessary precautions to prevent the theft of equipment (such as laptops, tablets) to avoid disclosure of personal information to unauthorized persons.
- Avoid discussing personal information in public places such as lobbies, elevators, restaurants, train stations and airplanes. Discuss issues about an identifiable individual behind closed doors and refrain from using speakerphones.
- Personal information is particularly vulnerable at the time of destruction. Ensure that both paper and electronic media containing personal information are fully destroyed beyond recovery before they leave your secure custody.
- Avoid copying or retaining records on the sole basis of convenience or "just in case" logic; make sure copies are destroyed quickly and securely.
- Retain and destroy master copies of records only in accordance with pre-determined retention periods and documented scheduling processes. Don't destroy information that is the subject of a current request for access.

Fax and email security tips

Fax and email are not very secure methods for transmitting health information, yet their use is widespread. Here are some tips for make these transmissions as secure as possible:

For all transmissions

- Limit use to circumstances where it is immediately necessary for time-sensitive or functional reasons and to the least amount of information possible.
- Include a banner or notice about the confidentiality of the information and a contact should the information be received in error.

For fax transmissions

- Confirm fax number by phone before sending transmission.
- Ensure that the recipient's machine is in a secure area. Otherwise, the recipient should stand by to receive and confirm transmission of the information.
- Use a cover sheet.
- Confirm the number being dialed by visual check on the fax machine display. For frequently dialed numbers, use the automatic dialing feature to minimize incorrect dialing.
- Print out and check the fax machine logs after transmission to verify that documents were received at the correct number.
- If it is determined that the transmission was received by a wrong number: (a) contact the recipient and ask them to return or destroy the documents, (b) retain copies of all information sent, and (c) report the incident as an information security breach.
- Post these procedures at every fax machine in your area.

For email transmissions

- Do not transmit identifiable personal information by email to an external or public network unless the information is secured by encryption.
- Do not include identifiers or personal information in the subject header of the mail.
- Verify all addresses as correct before sending messages.
- Request notification of receipt.

Service provider agreements

A pharmacy professional that outsources or contracts with an outside agency for health services or information management services must ensure that the service provider's practices are compliant with the HIA. The service provider should have in place polices and processes that meet relevant privacy and security standards. Both parties are obligated to meet these standards in their service agreements.

Privacy breach responses

Your response to a privacy breach is as important as the measures you have in place to prevent one. Here are some general steps to follow in responding to a privacy breach:

- Report the incident immediately to the Privacy Officer, who should direct the response.
- Confirm the breach or violation and the level of gravity or potential for harm.
- Take all necessary steps to prevent further breach of the information, including retrieval of breached records from any unauthorized recipients.
- Investigate thoroughly the nature and cause of the breach and develop measures to prevent them in the future.
- Decide whether the subjects of the breach should be notified. Do not inform the subject if it is determined that disclosure of the breach would likely harm the subject. Factors favouring notification include
    - it is evident that the breach presents a danger to the subject;
    - the breached information cannot be retrieved or destroyed;
    - the quantity of information and subjects involved in the breach are significant;
    - the recipient of the breach has or is likely to contact the subject;
    - the subjects are likely to be informed by other means.

Important update

As of August 31, 2018, health custodians in Alberta are required to report privacy breaches. Find more information here.

8. Commissioner's investigations and orders

Below are summaries of investigative reports and orders issued by the Information and Privacy Commissioner of Alberta relating to pharmacy professionals.

The Medicine Shoppe (Investigation Report H2002-IR-002), Nov. 25, 2002

http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2224

Complaint:
Pharmacist disclosed a list of past medications issued to a patient to the patient's estranged husband (unknown to the pharmacist at the time). Request came around income tax time so pharmacist assumed it was for tax purposes.

Finding:
The pharmacist's disclosure of the complainant's health information was in contravention of the HIA, since it was not by the patient's consent, nor was the husband an authorized representative of the patient. The disclosure also went beyond provisions allowing disclosure to family or friends of limited and current information. The investigator also found that the pharmacist had not instituted measures and policies to properly protect the confidentiality of health information under their custody and control.

Wal-Mart Canada (Investigation Report H2006-IR-001), Feb. 2, 2006

http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2243

Complaint:
Pharmacist required that the patient provide personal information to purchase insulin.

Finding:
The pharmacist's practice of collecting the prospective purchaser's name, address, date of birth and phone number and relevant information pertaining to any allergies or medical conditions for the sale of insulin is for an authorized purpose (provision of health services) under the HIA.

Drugstore Pharmacy, Real Canadian Superstore (Order H2007-002), Jan. 31, 2008

http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2249

Complaint:
Pharmacist's request to show driver's licence to verify purchase of Schedule 2 drug.

Finding:
Since the driver's licence information was only viewed, not recorded, the collection was not in contravention of the HIA.

Pharmacist (Investigation Report H2008-IR-001), May 15, 2008

http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2256

Complaint:
Patient did not want her health information disclosed and entered on Alberta Netcare PIN database. Her pharmacist was told that submission of her data to Netcare was mandatory. Alberta Health would not accommodate her request.

Finding:
Alberta Health is the custodian of Alberta Netcare and, in line with HIA s.58(2), did not consider and accommodate when appropriate the expressed wishes by the patient to limit disclosure of her health information. Alberta Health must implement and make available to patients a Global Person Level Masking option at point of collection.

Pharmacist (Investigation Report ???), Dec. 6, 2011

http://www.oipc.ab.ca/Content_Files/Files/News/NR_Prosecution.pdf

Complaint:
Pharmacist inappropriately accessed an individual's health information using Alberta Netcare for reasons other than providing a health service and posted information about a prescription medication she had taken to Facebook.

Finding:
The pharmacist was charged with knowingly obtaining or attempting to obtain health information in contravention of the HIA and was fined $15,000.

Calgary Co-op (Investigation Report H2012-IR-001), Oct. 4, 2012

http://www.oipc.ab.ca/downloads/documentloader.ashx?id=3107

Complaint:
Patient objected to the collection of information about immune system conditions on a form that he was told he needed to complete before his prescribed B12 injection would be administered.

Finding:
Information as to whether or not a patient's immune system is compromised is not clinically relevant to the decision to administer a vitamin B12 injection. The pharmacy's practice of collecting immune system function information on every patient seeking injection contravenes the requirements HIA s.58(1) as it was not sufficiently limited.

9. Definitions

Affiliate
An employee, volunteer, agent, outsourced service provider, or information manager (subject to additional conditions) completing activities on behalf of a custodian.

Authorized representative
A person who has been assigned to represent another individual, and to exercise the rights of the individual on their behalf. Persons recognized as having this status varies with the legislation, but generally includes

- guardian of a minor 18 years or younger who is not competent to understand his or her rights;
- personal representative for the administration of a deceased individual's estate;
- guardian or trustee under the *Adult Guardianship and Trusteeship Act*;
- agent under the *Personal Directives Act*;
- attorney under power of attorney;
- nearest relative of a formal patient under the *Mental Health Act*; or
- person with written authorization from the individual to act on the individual's behalf.

Collection
Acquiring or receiving information into an organization's custody and control.

Confidentiality
Confidentiality is a condition under which information is not disclosed by a person or organization to others. Preserving confidentiality is one means by which an organization protects the privacy of individuals.

Custody and control
Custody means having physical possession of the information in situations where you have the ability to deal with the information. Control means having the authority and/or responsibility to manage the information, including making decisions on access, use, disclosure and disposition. Generally, information you create or receive as part of your mandated activities or functions is under your control. Note that you may still have control over information that is not in your custody.

Custodian
An organization or health professional designated under the HIA that is subject to the obligations and powers set out in the HIA. Custodians under the HIA are identified as Alberta Health Services, Alberta Health, nursing homes, licensed pharmacies, ambulance operators, as well as health professionals who are registered members of

- Alberta College of Pharmacy,
- Alberta College of Optometrists,
- Alberta Opticians Association,
- Alberta College and Association of Chiropractors,
- College of Physicians & Surgeons of Alberta,
- Alberta Association of Midwives,
- Alberta Podiatry Association,
- College of Alberta Denturists,
- Alberta Dental Association and College,

- College of Registered Dental Hygienists of Alberta, and
- College and Association of Registered Nurses of Alberta

Custodians are responsible to comply with the HIA for any health information under their custody and control. This includes all health information they or their affiliates collect, receive, or disclose as part of the custodian's mandated functions and operations.

Disclosure
Release of information to individuals or agencies outside of the organization, or to individuals within the organization that are not authorized to access the information according to authorized purposes outlined in HIA s.27. Does not include release of information in response to a right of access request.

Health information
Any or all of the following
- diagnostic, treatment, and care information;
- registration information.

Information manager
A person or agency acting as an affiliate to a custodian that
- processes, stores, retrieves or disposes of health information;
- strips, encodes or otherwise transforms individually identifying health information to create non-identifying information; or
- provides information management or information technology services.

HIA s.66 requires that custodians have an agreement with the information manager that sets out terms for collection, use, disclosure, access and security of health information handled by the information manager on behalf of the custodian.

Masking
In electronic health records systems such as Netcare, measures to ensure that some or all authorized users of a shared database do not see any or part of the information about specific individuals that is resident in the system. This technique is used to accommodate individual requests for limiting disclosure under HIA s.56.4 and 58.

Pharmacy professionals
Registrants of the Alberta College of Pharmacy.

Privacy
Privacy is the right to be left alone. In practical terms, it is the ability of individuals to control access to their personal information in the custody or under the control of others through accountability, consent, security, right or access, and regulation.

Privacy breach
An unauthorized collection, use, disclosure, destruction, or modification of personal information.

Privacy Impact Assessment (PIA)
A formal, documented assessment of the privacy risks involved in introducing new information systems, practices, or policies for handling personal information. As required under HIA s.64, PIAs must be completed by the custodian and submitted to the Office of the Information and Privacy Commissioner of Alberta for review and comment before implementation of the new system, practice, or policy. The Commissioner has

developed requirements and guidelines for completing and submitting a PIA.

Research
Academic, applied, or scientific study that necessitates the use of individually identifying health information.

Security
The processes, tools and measures used to identify threats and risks to the confidentiality or integrity of information, and to implement administrative, physical and technological means to combat identified threats and risks.

Use
Release or sharing of information within the organization for purposes outlined in HIA s.27.

10. Resources

Legislation

Health Information Act, RSA 2000, C. H-5
Designation Regulation (*Health Information Act*), AB Reg. 69/2010
Health Information Regulation, AB Reg. 70/2001
Alberta Electronic Health Record Regulation, AB Reg. 118/2010

Alberta Health

Health Information Act Help Desk (during business hours)
Phone: 780-427-8089 or toll free by first calling 310-0000

Health Information Act Guidelines and Practices Manual *(does not include 2010 amendments)*

Office of the Information and Privacy Commissioner of Alberta

Information and Privacy Commissioner of Alberta
410, 9925 - 109 St.
Edmonton, AB T5K 2J8
Phone: 780-422-6860 or toll free at 1-888-878-4044
Fax: 780-422-5682
E-mail: generalinfo@oipc.ab.ca
Web: http://www.oipc.ab.ca

Health Information - A Personal Matter: A Practical Guide to the *Health Information Act*

11. Appendices

Appendix 1: Sample notification for collection of health information

Appendix 2: Form for authorized consent under the HIA

Appendix 1: Sample notification for collection of health information

Your health information at this pharmacy:

What you need to know

Your health information at our pharmacy is protected under the *Health Information Act*.

We will collect and use your health information only to support the health services we provide to you:

- Providing safe and effective service and care,
- Verifying your eligibility for health services,
- Conducting investigations or reviews of practice,
- Completing research under ethical review,
- Supporting health provider education, or
- For internal management purposes, such as billing, insurance claims, and audits

We will not disclose your health information to non-healthcare agencies without your consent.

Except in special family or emergency circumstances, you will be asked for your consent before we give your information to anyone other than another health agency involved in your care.

We have measures in place to protect your health information from unauthorized disclosure or loss.

For more information, please ask us or our Privacy Officer at:

privacy@abpharmacy.ca

Appendix 2: Form for authorized consent under the HIA

Consent for the Disclosure of Health Information

I, _____, consent to the release of
(Name)

_____
(Identify nature of personal information)

_____

to _____
(Identify individual/organization to whom information may be released)

for the purpose of _____
(Indicate how information will be used/disclosed)

_____

_____

- I have been made aware of the reasons for the disclosure of the above information, and the risks and benefits associated with consenting or not consenting to its release.
- I understand that I may revoke my consent at any time by providing a signed, written statement to the custodian of the information.

Signature: _____ Date: _____

Print name: _____ Valid until: _____