

HEALTH INFORMATION ACT

Guide to Policies and Procedures

For Physician Offices



February 2003

Table of contents



INTRODUCTION

The <i>Health Information Act</i> applies to you!	4
You must have a policy and procedure manual	5
A worthwhile activity	6
About this guide	7
Other resources	8
About the sponsors	9



TOPICS FOR YOUR POLICY AND PROCEDURE MANUAL:

Format for your policy statements	11
Content for your policy statements	12
Policy topic: Roles and responsibilities	13
Policy topic: Right of access	15
Policy topic: Information handling and security	20
Policy topic: Collection, use and disclosure of health information	24
Policy topic: Information privacy and security in contracting	27
Policy topic: Research	29
Policy topic: Transitory records	31



ATTACHMENTS

Attachment one: HIA definitions	34
Attachment two: Sample policy statement outline	36
Attachment three: Sample form: request to access health information	38
Attachment four: Regulated fee schedule under HIA	40
Attachment five: Sample form: request to correct or amend health information	41
Attachment six: Sample form: confidentiality agreement	43
Attachment seven: Sample mini-poster regarding purpose and authority for collection of health information	44
Attachment eight: Section 42 notice to recipient to accompany disclosure (with consent)	45
Attachment nine: Section 42 notice to recipient to accompany disclosure (without consent)	46
Attachment ten: Sample form: consent to the disclosure of individually identifying health information	47
Attachment eleven: Checklist of components for agreement with Information Manager	49
Attachment twelve: Sample research agreement	52



Introduction

The *Health Information Act* applies to you!



Alberta's *Health Information Act* (HIA) came into force April 25, 2001, and applies to health information held by custodians and their affiliates – whether you work in paper-based or computerized practice. The HIA outlines the legal responsibilities of custodians with respect to health information in their custody or control.

For the most part, physicians in private practice are considered custodians. Staff or contractors of those practices are usually considered affiliates.

What does this mean? It means the *Health Information Act* applies to you.

You must have a policy and procedure manual



The HIA says that **every physician office must have a written policy and procedure manual relating to how you handle health information.** You and your staff have always taken patient privacy seriously, so you probably already have many excellent policies and procedures in place. **The difference is, now you must have them written down.** And, some of your existing procedures may need some adjustment to comply with the letter of the law under HIA.

The Privacy Commissioner can conduct an investigation of how health information is handled in your office – how you as a custodian, and the staff affiliates for whom you are responsible, deal with privacy in your practice.

When such reviews occur, the first thing the commissioner will ask to see is your policy and procedure manual. That's where this guide comes in. It will:

- Walk you through what's required to become compliant with HIA
- Help you clarify exactly what your policies and procedures are
- Show you how to write those policies down

A worthwhile activity



It will take some time to work through this manual and develop your policies and procedures. Doing so, however, is a very worthwhile exercise that will help you ensure you are doing all you can to protect your patients' privacy. And, developing your policies and procedures will help you become compliant with HIA. The HIA is law and this guide will help you learn to live with it – while providing some good advice for information handling in general.

In today's age of technology and electronic communications, patients have concerns about how their information is collected, used, disclosed and safeguarded. Documenting and communicating information to your office team about privacy and security policies and procedures demonstrates that you are committed to protecting the confidentiality of health information and maintaining the privacy of your patients and staff.

About this guide



Under HIA, physicians as custodians have some primary responsibilities:

- You (custodian) must establish or adopt policies and procedures to implement the act and the regulations (section 63).
- You (custodian) must take reasonable steps to maintain administrative, technical and physical safeguards that will protect the confidentiality of health information in your custody or control and the privacy of your patients (section 60).

The *Health Information Act Guide to Policies and Procedures for Physician Offices* has been developed specifically to assist you to meet these legislated responsibilities under the act, whether you work in a paper-based or computerized practice.

Much of the content for this guide is quoted directly from the act. We have tried to simplify as much as possible, but there are times when the “letter of the law” will be your best bet.

Please note that the HIA also requires you to prepare a privacy impact assessment (PIA) when proposing to make changes to administrative practices and information systems (computers, physical storage or paper files, etc.) relating to the collection, use and disclosure of individually identifying health information. Your PIA describes how proposed changes may affect the privacy of the individual who is the subject of the information (section 64).

- **PIAs are not covered in this guide.** If you need assistance conducting a PIA, or for more information, see the *Alberta Medical Association/Physician Office System Program Guide to Privacy Impact Assessments*.

Other resources



The *Guide to Policies and Procedures* provides general information about developing information privacy and security policies and procedures for your office.

For further information about HIA, be sure to consult some of the resources available:

- *Health Information Act: Making it work. AMA and College of Physicians and Surgeons of Alberta Guide for Medical Office Staff*, November 2001

www.albertadoctors.org/advocacy/healthinfo/index.html or call AMA Public Affairs (780) 482-2626, toll-free 1-800-272-9680

- *Health Information, A Personal Matter*. Office of the Information and Privacy Commissioner (OIPC), 2001

Available through the Queen's Printer

Edmonton Phone: (780) 427-4952 Fax: (780) 452-0668

Calgary Phone: (403) 297-6251 Fax: (403) 297-8450

OIPC website: www.oipc.ab.ca

- *Health Information Act: Guidelines and Practices*, Alberta Health and Wellness, 2001
www.health.gov.ab.ca/public/document/HealthInformationAct/guidelines2.pdf

- *Health Information Act*, Queen's Printer online
www.qp.gov.ab.ca/documents/acts/H05.cfm



For some commonly used HIA definitions, see Attachment one.

For a summary of your fundamental ethical requirements regarding protection of patient privacy, with or without the HIA, see the Canadian Medical Association Code of Ethics (www.cma.ca click "Inside CMA," then "Where We Stand," then "Code of Ethics").

For information on College of Physicians and Surgeons of Alberta requirements for health records and information, see:

- *Office Medical Records – CPSA Guideline*
- *Release of Medical Information: A Guide for Alberta Physicians*

Both available www.cpsa.ab.ca

About the sponsors



This guide is brought to you by the Alberta Medical Association (AMA), courtesy of the Physician Office System Program (POSP).

POSP is a joint AMA and Alberta Health and Wellness (AHW) program providing financial support and change management services for implementation of computer technology in physician practices. This guide was created initially to support program participants.

The AMA is sponsoring adaptation of this guide and its distribution to all physicians.

Every physician in Alberta – with or without participation in POSP – has certain duties to perform under HIA. As discussed in the introduction, this guide will help you understand what must be done in your office.

We gratefully acknowledge the invaluable assistance of the Office of the Information and Privacy Commissioner, the College of Physicians and Surgeons of Alberta and privacy consultants Denham & Associates.



Topics for your policy and procedure manual

Format for your policy statements



You can record your policy statement information in whatever way works best for you and your staff. There is no “approved” format. To help you get started, though, Attachment Two provides a suggested format and tells you what such a policy statement should include.



2

Please review Attachment Two now.

Content for your policy statements




Now that you've seen what a policy statement typically includes, you are ready to begin thinking about what your individual policies or procedures should be, and what they should include.

We suggest that you will probably need at least seven policy statements. You may decide you need more, but at a minimum, your policy and procedure manual should contain:

- Roles and responsibilities
- Right of access
- Information handling and security
- Collection, use and disclosure of health information
- Information privacy and security in contracting
- Research
- Transitory records

These seven topics are addressed in the remainder of this guide. Each topic section begins with *Background*. It tells you what part of the HIA applies to the topic. Next comes the *Policy Content* section, that tells you what content should be included in your office's policy or procedure for the particular topic.

We have marked this section with  so that you can see that this is the section where your work must be done.



In some cases, you can take the text you find there and reproduce it directly in your own manual. In some cases, there are decisions you must make and activities required before you can spell out what your policy will be. Please read the Policy Content section carefully.

Policy topic: Roles and responsibilities



BACKGROUND

Under section 62 of the HIA, you (the custodian) are required to identify:

- an individual in your office who will be responsible for ensuring compliance with the act and your privacy and security policies and procedures

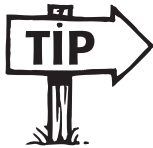


POLICY CONTENT

Your **roles and responsibility policy** should:

1. Identify an individual to act as a privacy contact for HIA matters. This may be you or another physician. In most practices, however, the privacy contact will be a staff person, clinic manager or administrator.

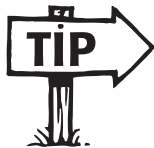
Please note: Designating an individual in the practice to be the privacy contact does not affect or pass on your professional obligations under the Code of Ethics (See Other Resources).



When you state which individual in your office will be designated to act as the privacy contact, identify the position (e.g., Clinic Manager), not the name of the individual. Then, if your clinic experiences staff turnover, you will not have to update your policies.

2. Document the factors you consider when designating this individual:
 - Does he/she have an interest in privacy?
 - Is he/she a full-time employee, or part-time? Who will provide back-up if he/she is away?
 - **How will you (and your partners, if applicable) work with the privacy contact? How will you support each other? If you work in a larger clinic, would it be helpful to establish a representative committee made up of other staff members?**
3. Describe the responsibilities of the privacy contact. These may include some or all of the following:
 - identifying privacy compliance issues for the practice
 - ensuring that privacy and security policies and procedures are developed and maintained
 - ensuring that all staff, students, volunteers and contracted personnel are aware of their duties, roles, and responsibilities under applicable privacy legislation

- providing advice to physicians and staff regarding release or non-release of health information (stored within medical records in your office)
 - responding to requests for access to information, or to correct or amend health information
 - ensuring the overall security and protection of health information throughout the practice
 - ensuring the proper retention and disposal of health information
 - acting as a contact when dealing with the Alberta Office of the Information and Privacy Commissioner (OIPC)
4. Include related statements that apply to ALL staff:
- All staff are responsible for:
 - a) protecting the confidentiality of any health information they may have access to through the performance of their job duties
 - b) collecting, using and disclosing health information only in the performance of their job duties
 - c) reading and signing-off on privacy and security policies and procedures
 - d) reporting privacy breaches to the privacy contact
 - e) other



These general responsibilities can also be added to existing job descriptions.

5. Include a statement that physicians in the practice adhere to the Canadian Medical Association Code of Ethics, including their fundamental responsibility to protect patient privacy.

Policy topic: Right of access



BACKGROUND

Section 7 of the HIA states that:

- Individuals have a right to access health records about themselves, with a few limited and specific exceptions.

Section 13 states that:

- Individuals who believe there is an error or omission in their health information may request that the information be corrected or amended.



POLICY CONTENT

A right of access policy identifies and documents (i) how you manage requests and help patients access their own health information and (ii) how you handle requests to correct or amend health information.

Your **right of access policy** should:

1. State how you handle informal requests for access to health information

Consider the kind of requests you receive now and how often you receive them. Most common requests for health information are likely from patients.

In your policy explain how your office will handle informal requests. Different offices might have different policies, but all should be HIA compliant.

Requests from patients to access their own basic health information

You might state, for example:

- Requests from individuals to access basic health information about themselves (e.g., confirm a diagnosis, check on lab results, etc.) are a routine release of information with valid identification.

Or,

- Diagnostic results or diagnoses are handled only by the physician. Staff do not provide results.

Requests from patients to correct or amend their own basic health registration information (e.g., change of address, correct a Personal Health Number)

You might state:

- Patient requests to correct or amend basic health registration information about themselves are handled informally with presentation of valid documentation (e.g., driver's license, Alberta Health Care Insurance Plan card).

Requests for access from someone other than the patient (the husband or wife of a patient, the parent of a minor patient, or a family member of a deceased individual)

Section 104 of the HIA specifies others who may exercise the individual's right of access. Identify these people in your **right of access policy** by quoting from the act as follows:

"The following persons may exercise any right or power conferred on the individual under the *Health Information Act*, including the individual's right of access to his/her own health information, or to correct or amend health information:

- a) if the individual is 18 years of age or older, by the individual
- b) if the individual is under 18 years of age and understands the nature of the right or power and the consequences of exercising the right or power, by the individual
- c) if the individual is under 18 years of age but does not meet the criterion in clause (b), by the guardian of the individual
- d) if the individual is deceased and was 18 years of age or over immediately before death, by the individual's personal representative (e.g., administrator or executor) if the exercise of the right or power relates to the administration of the individual's estate
- e) if a guardian or trustee has been appointed for the individual under the *Dependent Adults Act*, by the guardian or trustee if the exercise of the right or power relates to the powers and duties of the guardian or trustee
- f) if an agent has been designated under a personal directive under the *Personal Directives Act*, by the agent if the directive so authorizes
- g) if a power of attorney has been granted by the individual, by the attorney if the exercise of the right or power relates to the powers and duties conferred by the power of attorney
- h) if the individual is a formal patient as defined in the *Mental Health Act*, by the individual's nearest relative as defined in the Act if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act, or
- i) by any person with written authorization from the individual to act on the individual's behalf"

Decide what documentation you require when a substitute decision maker wants to access or amend health information. Explain this in your policy. For example:

- staff will carefully review documentation provided by the applicant to ensure they have authority to act on behalf of the individual

Specify in your policy if it is the applicant's responsibility to provide documentation proving he or she is an individual's substitute decision maker.

*Finally, you may want to include the following statements in the general provisions of your **right of access policy**:*

- Every reasonable effort to assist the applicant and to respond openly, accurately and completely shall be made. This includes providing an explanation of any term, code or abbreviation used in the record.
- A record must be created from information in electronic form if
 - a) required to provide a response to the applicant
 - b) doing so involves using normal computer hardware, software and technical expertise, and
 - c) it would not unreasonably interfere with the clinic's operations

2. State how you will handle formal requests for access to health information

Occasionally you may receive a request for health information that cannot be handled informally (e.g., when a large volume of records is requested, such as the entire patient chart).

- Explain your procedure for handling these requests. We suggest the following based on the HIA wording in sections 8 – 12. You can customize it for your own practice.

 3

- You can require requests for access to information to be in writing (see Attachment Three). A person may request access to another person's information only if he or she has that person's signed consent, or proof of authority to act on the other person's behalf under section 104 (see previous page).

- All requests for access to information should be directed to the privacy contact.

 4

- After receiving the request, the privacy contact will retrieve the requested records and, in accordance with the fee schedules set out in the HIA, prepare a fee estimate (see Attachment Four).

- Once the fee estimate is prepared, the privacy contact will notify the applicant of the cost for providing the information requested. The applicant has up to 20 days to indicate if the fee estimate is accepted or to modify the request to change the amount of fees assessed.

- Processing a request ceases once a notice of estimate has been forwarded to an applicant and begins again immediately on the receipt of an agreement to pay the fee, and on the receipt of at least 50% of any estimated fee. (Note: The act allows you to request a deposit, but you do not have to require one.)

- Once the estimate has been accepted by the applicant, the privacy contact will review the requested records and, in consultation with appropriate staff (e.g., the responsible physician) prepare the records for disclosure. All records relating to the request will be reviewed on a line-by-line basis to determine possible exceptions to disclosure.

- Access to health information cannot usually be denied based on the reason stated by the applicant for the request. In some cases, the privacy contact may determine that discretionary or mandatory exceptions apply to the records requested.

- Health information **must not be disclosed** to an applicant

- a) if it is about an individual other than the applicant, unless
 - i. it was originally provided by the applicant in the context of receiving a health service, or
 - ii. the applicant has authority under section 104 of the HIA to receive the information (See page 16)
- b) if it sets out procedures or contains results of an investigation, discipline proceeding, practice review or an inspection related to a health services provider
- c) if the disclosure is prohibited by legislation

- Health information may not be disclosed to the applicant if the disclosure could reasonably
 - a) threaten the health or safety of another individual or the public
 - b) lead to the identification of a person who provided health information in confidence
 - c) be expected to prejudice the use or results of audits, diagnostic tests or assessments.
- In such instances the excepted information will be removed (severed) from the record prior to the record being disclosed to the applicant. The applicant will be advised that information has been severed, and under what sections of the HIA the exceptions have been made.
- Response to the applicant must be made within 30 days of receipt of the request unless the time limit has been extended as allowable by law.
- As part of the response, the applicant will be told:
 - a) whether access to the record or partial record is granted or refused
 - b) if access is granted, where, when and how access will be given, and
 - c) if access is refused:
 - i) the reasons for refusal and basis of refusal
 - ii) the name, title, business address and phone number of the privacy contact, and
 - iii) that the applicant has a right to request a review of the decision by the Alberta information and privacy commissioner.
- A staff member shall be present if the applicant views the original record to answer questions and maintain the integrity of the record. If information is severed from the record before disclosure of the information, the applicant no longer has the option of viewing the entire original record.

3. State how you will handle formal requests to correct or amend health information

Some requests to correct or amend health information cannot be handled informally. For example, a patient may dispute that he/she was taking a medication, or was diagnosed with a particular condition.

You may want a written procedure for handling these requests. The following wording is based on sections 13-15 of the HIA but can be customized:



5

- Requests to correct or amend information must be in writing (Attachment Five). An individual may request a correction to another person's information only if they have authority to act on the other person's behalf under section 104 (see page 16).
- The privacy contact will review the request and consult with appropriate staff members (e.g., physicians) to determine whether the request is to be granted or refused. Corrections will only be made to factual based information and will not apply to opinions. The correction process must be completed within 30 days of receipt of the request for correction, unless the time has been extended as allowable by law.

- In the case of a correction, the privacy contact shall ensure that the correction is made, and inform the applicant in writing.
- In the case of a refusal to correct or amend the information, the privacy contact shall inform the individual that they may
 - a) ask for a review of this decision by the Alberta Information and Privacy Commissioner,
 - or
 - b) submit a statement of disagreement setting out in 500 words or less the requested correction or amendment and the applicant's reasons for disagreeing with the decision.
- If the applicant elects to submit a statement of disagreement, the statement shall be attached (if reasonably practicable) to the information that is the subject of the request for correction or amendment. Any person to whom the record has been disclosed in the past year shall receive a copy of the statement of disagreement.
- The privacy contact will advise any person to whom the information was disclosed in the preceding year that a correction or amendment has been made. The only exceptions are:
 - a) the custodian agrees to make the correction or amendment but believes the applicant will not be harmed if notification is not provided (section 13(4)).
 - b) the applicant agrees.

Policy topic: Information handling and security



BACKGROUND

Under section 60 of the HIA, custodians are required to take reasonable steps to maintain administrative, technical and physical safeguards to protect the confidentiality of health information, and patient privacy. This includes protection against unauthorized use, disclosure, access to, or modification of the health information.

In addition, section 8 of the regulations states that custodians must:

- Identify and maintain a written record of all administrative, technical and physical safeguards you have in place to protect health information
- Periodically assess these safeguards to ensure their continued effectiveness
- Designate an individual to be responsible for overall security and protection of health information
- Ensure that staff are aware of, and adhere to, all administrative, technical and physical safeguards
- Establish penalties that may be imposed against anyone who breaches or attempts to breach safeguards
- Before storing information in a jurisdiction outside of Alberta, allowing a person outside of Alberta to use information or disclosing information to such a person, enter into a written agreement that ensures the information is adequately safeguarded (regulation 8(4)).



POLICY CONTENT

Your **information handling and security policy** should include some, or all, of the following statements as they apply to your practice:

1. Relating to administrative safeguards
 - Information privacy and security policies and procedures have been developed and are updated as necessary.
 - Only the least amount of information necessary for the intended purpose is collected, used and disclosed.
 - Access to health information is restricted to staff who require access to the information in order to perform their job duties.
 - 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.

6 

- Staff are monitored for compliance with privacy and security policies and procedures.
- All new staff are required to review the privacy and security policies and procedures, and to sign off that they have read, understood, and will abide by them.
- All staff are required to attend privacy and security training sessions on a _____ basis.
- All staff, students, volunteers, and contracted personnel (e.g., janitors, temporary staff, etc.) are required to sign a Confidentiality Agreement (Attachment Six).
- Confidential information is not transmitted verbally if conversations can be overheard or intercepted.
- Patients and visitors are accompanied by a staff member to private or semi-private areas such as examination rooms and/or physician offices.
- Before implementing any new administrative practice or information system related to the collection, use and disclosure of health information, a privacy impact assessment (PIA) is completed and submitted to the Office of the Information and Privacy Commissioner (OIPC) (See page 7).
- All privacy compliance issues and security breaches are reported to the privacy contact.
- Health information is retained in accordance with the records retention provisions stated in the Physicians' Office Medical Records Policy of the College of Physicians and Surgeons of Alberta (currently under review by CPSA).
- HIA obligations are clearly passed along by contracts with information managers, researchers, contractors and recipients outside Alberta.

2. Relating to technical safeguards

- All paper or electronic information systems users are assigned a unique identifier (User ID) that restricts access to health information and systems that are required for the administration of their duties.
- Access to electronic health information systems is password protected.
- Passwords are kept confidential at all times and are not to be written down, posted publicly, or shared with other staff.
- Passwords are changed every _____ months.
- Screen saver passwords are used to protect against unauthorized access if a computer is left unattended.
- Confidential information sent via email over public or external networks is encrypted.
- Information systems are audited to detect unauthorized access and prevent modification or misuse of health information.
- Audit trails are reviewed every _____ months, and on an incident basis.
- Health information is protected from unauthorized external access by a firewall.
- Virus scanning software is installed to protect health information from unauthorized modification, loss, access or disclosure.

- Electronic health information systems are backed up on a _____ basis.
- Back-up information is stored in a secure, locked environment off-site.
- Information intended for long-term storage on electronic media (e.g., tape, DVD, disk) is reviewed on an annual basis to ensure the data is retrievable, and to migrate the data to another storage medium if necessary.

3. Relating to physical safeguards

- Clinic records, both on-site and off-site, are held and stored in an organized, safe and secure manner.
- Paper-copy patient charts are labeled using a code, instead of a patient name.
- Rooms and cabinets used to store health information are locked when not in use.
- Records storage areas are equipped with smoke detectors, fire extinguishers and sprinkler systems when possible.
- The distribution of keys is strictly controlled; keys are returned by staff after their employment has been terminated.
- Building premises are protected by building alarms. Alarm codes are changed every _____ months.
- Patient information is not left unattended in areas to which the public has access.
- Computer monitors are positioned so that on-screen information cannot be viewed by passers-by.
- The electronic health information system's network server is located in a locked room.
- Privacy screens are used where necessary to prevent individuals from viewing confidential information unless looking directly at the screen.
- When health information is transported to another location, it is placed in a sealed envelope, marked as confidential, and directed to the attention of the authorized recipient.
- Clinic staff verify the identity and credentials of courier services used for the transportation of health information.
- Patient charts that are left outside physician examining rooms are turned so that the patient's name is not visible.
- Patient charts are not to be removed from the building premises.
- Fax machines are located in a secure area.
- Preprogrammed numbers are used to send fax transmissions.
- Preprogrammed numbers are reviewed every _____ months to ensure they are still accurate.
- All fax transmissions are sent with a cover sheet that indicates the information being sent is confidential.
- Reasonable steps are taken to confirm that health information transmitted via fax is sent to a secure fax machine, and to confirm that the information was received.

- Health information in paper format is disposed of by confidential shredding.
- Destruction is documented by listing the records/files to be destroyed, recording the date of destruction, and having a staff member sign off that the destruction occurred.
- All information is wiped clean prior to disposal of electronic data storage devices (e.g., surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMS, etc.), or the device(s) are destroyed.

4. Security breaches

Your **information handling and security policy** may also include some provisions addressing how you handle security breaches or other compliance issues. For example:

- All security breaches or privacy compliance issues are reported to the privacy contact.
- The privacy contact will investigate the breach and evaluate the severity based on the degree of harm to the individuals involved, the sensitivity of the information, and the degree of malicious intent. Additional staff will be involved in the investigation as necessary to determine the cause of the breach and to implement any corrective or disciplinary actions required.
- Depending on the nature and severity of the breach, the privacy contact will notify the OIPC that a breach has occurred.
- The results of the investigation will be communicated to appropriate staff (physicians, supervisory/managerial staff), and corrective action will be taken.
- Any applicable sanctions will be applied by the appropriate supervisory/managerial staff.

Policy topic: Collection, use and disclosure of health information



BACKGROUND

Section 27 of the HIA outlines authorized uses of health information; sections 35–37 describe authorized disclosures of health information.

Collection: The process of gathering health information from an individual

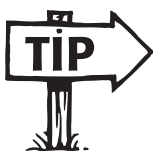
Use: What you do with health information once you've collected it, including reproduction (but not disclosure)

Disclosure: Providing health information to other custodians or to outside parties

Health information can be collected and used only for the following purposes authorized under the HIA:

- a) to provide health services
- b) to assess an individual's eligibility to receive a health service
- c) to conduct investigations, discipline proceedings, practice reviews or inspections
- d) to conduct research (with the approval of an appropriate ethics committee)
- e) to provide education for health service providers
- f) to carry out a purpose authorized or required by legislation (e.g., *Public Health Act*, *Child Welfare Act*, *Cancer Programs Act*, etc.)
- g) for internal management purposes, including planning, resource allocation, policy development, quality improvement/quality assurance, monitoring, audits, evaluation, reporting and to manage human resources
- h) to obtain or process payment for health services

Before disclosing, the HIA allows you to consider the express wishes of your patient and relevant factors under section 58(2). This allows the patient to specify if he/she does not wish certain pieces of health information to be shared. Section 58(1) also states that you should collect, use or disclose only the amount of health information that is essential for good care.



For information on College of Physicians and Surgeons of Alberta requirements, see *Release of Medical Information: A Guide for Alberta Physicians*.



POLICY CONTENT

Your **collection, use and disclosure of health information policy** should set out rules for the collection, use and disclosure of health information in your custody or control. The following are examples of policy statements that you may choose to include:

1. Collection and use of health information
 - Health information is collected directly from the individual who is the subject of the information, or his/her authorized representative, unless:
 - a) the individual consents to the indirect collection of the information
 - b) direct collection would compromise the interests of the individual, the purpose of collection, the accuracy of the information, or the safety of any other person
 - c) direct collection is not reasonably practicable
 - d) the information is collected for the purpose of compiling a family or genetic history in order to provide a health service to the individual
 - e) the information is collected to assess the individual's ability to participate in a program, or receive a benefit, product or health service
 - f) the information is collected to inform the Public Trustee or Public Guardian about clients or potential clients
 - g) the information is publicly available
 - Patients in the practice are informed of the purpose and authority for the collection of information, and the availability of the privacy contact to answer questions or concerns.



You may want to develop a poster and/or brochure to serve as the main method of communicating this information. Suggested text appears in Attachment Seven.

2. Disclosure of health information
 - Individually identifying health information may be disclosed **without consent** in the following circumstances (as authorized by section 35)(1)), which include:
 - i. to another custodian, or affiliate, for any authorized use of the information (see the list under *Background* of this policy topic)
 - ii. to a person who is responsible for providing continuing care and treatment to the individual
 - iii. to family members of the individual, or a close personal friend, if the information is provided in general terms and concerns the presence, location, condition, diagnosis, progress and prognosis of the individual on the day on which the information is disclosed, unless contrary to the expressed wishes of the individual
 - iv. to contact family members or a close personal friend of the individual, if the individual is injured, ill or deceased, unless contrary to the expressed wishes of the individual
 - v. to comply with a subpoena, warrant or court order

vi. to a law enforcement officer in order to investigate a life-threatening personal injury to the individual, unless contrary to the expressed wishes of the individual

- Patient health information may be disclosed to a health professional body under section 35(4) for the purpose of an investigation, discipline proceeding, practice review or inspection. In such cases, the health professional body must agree in writing not to disclose the information except as authorized by its governing legislation and to destroy the information at its earliest opportunity.
- Personal information about doctors in your practice can be disclosed without consent to a health professional body for the purpose of an investigation, a discipline proceeding, a practice review, or an inspection.
- When individually identifying diagnostic, treatment and care information is disclosed without consent (for the above non-direct-care situations), a notation must be made of the name of the person who received the information, the date and purpose of the disclosure, and a description of the information disclosed. This notation of disclosure (e.g., copy of cover letter, log, etc.) must be retained for 10 years after the disclosure.
- Patient **consent is required** for all other disclosures of individually identifying health information, including release of information to insurance companies, lawyers, and employers.


8

- Attachment Eight contains a form that can be used as a notation record for your files and/or as a cover letter to *non-custodians* for disclosure of information with the patient's consent. (You do not have to complete this form when disclosing to another custodian.)


9

- Attachment Nine contains a form that can be used as (i) a notation record or (ii) a cover letter when disclosure occurs without the patient's consent.

3. Requirements of a valid consent

Your policy may also state the criteria for valid consent. For example:

- Under HIA, a consent for the release of health information must be in writing, and include the following information:
 - a) an authorization for the health information to be disclosed
 - b) the purpose for which the health information is disclosed
 - c) the identity of the person to whom the health information is disclosed
 - d) an acknowledgement that the individual providing the consent is aware of the reasons why the health information is needed and the risks and benefits of consenting or refusing to consent
 - e) the date the consent is effective and the date, if any, on which the consent expires
 - f) a statement that the consent may be revoked at any time by the individual providing it


10

Attachment Ten includes a sample Consent to the Disclosure of Individually Identifying Health Information form that can be customized for your practice.

Policy topic: Information privacy and security in contracting



BACKGROUND

Under section 60 of the HIA, you (custodian) must take reasonable steps to maintain administrative, technical and physical safeguards to protect health information and patient privacy. These responsibilities extend to health information that may be collected, used, disclosed or managed by an information manager or contracted service provider (e.g., electronic medical record vendor, computer vendor, third-party billing submitters, etc.).

The HIA requires custodians to enter into agreements in three situations: before disclosing health information to an information manager (section 66), to a researcher (section 54) or to a recipient outside of Alberta (regulations, section 8(4)).

To address these requirements, you may want to develop a policy around ensuring information privacy and security when contracting out services.



POLICY CONTENT

The following are policy statements you may want to include as part of your **information privacy and security in contracting policy**:

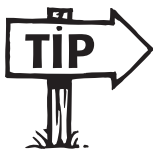
About your requirements as custodian

- An agreement or contract is completed and signed between the custodian and all contracted service providers who require access to the health information.
- Until a contract detailing information security provisions has been executed, the contracted service provider will not be allowed to access health information.
- When developing contracts with service providers who require access to health information provisions addressing the following are incorporated as required:
 - a) identifying the types of records provided, collected, created, or maintained in order to deliver the service
 - b) specifying any applicable privacy legislation (i.e., HIA, FOIP, any private sector legislation etc.)
 - c) identifying the organization(s)/company(ies) having custody and control of the records, including the responsibility and process for handling requests for access to information
 - d) ensuring that the contracted service provider meets or exceeds the standards set out in the custodian's information privacy security policies and procedures

- e) specify any audit or enforcement measures that the custodian will undertake to ensure that contracted service providers comply with information privacy and security provisions outlined in contractual agreements, e.g., non-disclosure agreements, audit trails, regular review of contracted service provider access requirements, inspection of contracted service provider premises.

About your service provider's requirements as contractor

- When developing contracts with service providers who require access to health information the service provider should address the following provisions (and you should state in **your** policy that you have asked the service provider to do so):
 - a) Ensure that the service provider's information security and privacy policies are available to you (custodian) upon request, including any updates or revisions that occur after execution of the contract
 - b) Document contracted service provider roles and responsibilities for carrying out specific information security processes
 - c) Ensure that employees of the service provider are aware of, and understand their responsibility to adhere to, your (custodian's) information privacy and security policies
 - d) Agree that the service provider and employees who have access to your (custodian's) information sign a confidentiality (non-disclosure) agreement
 - e) Agree to report breaches of confidentiality and privacy to you (custodian) within a specified time frame from the date of knowledge of the breach
 - f) Identify disaster recovery procedures and backup of any information assets and systems in the custody of the contracted service provider
 - g) Address the retention and disposition (e.g., destruction or return) of all information assets (e.g., records, hardware, system documentation) upon termination of the contract



As custodian, you must decide which provisions to include in agreements with contracted service providers. Some relationships may require more, or different, provisions than those listed here.



11

It is your responsibility to consult available sources, including legal counsel if necessary, to ensure that contract provisions are adequate to reduce or mitigate risks to privacy that may arise when contracting with outside service providers. See Attachment Eleven for components of an agreement with an information manager.

Policy topic: Research



BACKGROUND

Sections 48-56 of the HIA govern the collection, use and disclosure of individually identifying health information for research purposes. If you collect, use or disclose health information for research purposes, you should ensure that appropriate considerations and procedures for doing so are developed and documented.



POLICY CONTENT

You may want to include some or all of the following policy statements in your **research policy**:

- All requests for access to personal health information for research purposes must be in writing and accompanied by documentation indicating that the research proposal was reviewed and approved by an appropriate ethics committee.
- The following committees and boards are designated as ethics committees for this purpose:
 - a) Alberta Cancer Board – Research Ethics Committee
 - b) College of Physicians and Surgeons of Alberta – Research Ethics Review Committee
 - c) Alberta Heritage Foundation for Medical Research – Community Health Ethics Research Review Committee
 - d) University of Alberta – Health Research Ethics Board
 - e) University of Calgary – Conjoint Health Research Ethics Board
 - f) University of Lethbridge – Human Subject Research Committee
- Upon receipt of the request and ethics approval, you (custodian) **may** decide to disclose the health information to the researcher.
- If you (custodian) decide to disclose the health information, the researcher must agree to abide by any conditions suggested by the ethics committee or you (including obtaining any consents for disclosure that may be required).
- If you (custodian) decide to disclose health information for research purposes, the researcher must enter into an agreement with you in which the researcher agrees to:
 - a) comply with the provisions of the HIA and any applicable regulations
 - b) comply with any conditions imposed by you (custodian) regarding the use, protection, disclosure, return or disposal of the information
 - c) comply with any requirements to provide against identification of the subject individuals
 - d) use the health information only for the proposed research
 - e) ensure that the information is not published in any form that could lead to the identification of any of the subject individuals involved

- f) only contact individuals for additional information if the custodian has first obtained the individual's consent to being contacted for that purpose
- g) allow you (custodian) to access or inspect the researcher's premises to ensure that the researcher is complying with the terms set out in the agreement
- h) pay any costs levied by you (section 54(3))

12



An example of a research agreement is included as Attachment Twelve.

Policy topic: Transitory records



BACKGROUND

Transitory records are those documents that are required for routine or short-term transactions, and contain little or no information of ongoing value.

Appropriate use and maintenance of transitory records will help you to:

- a) ensure the most efficient use of office space and equipment by eliminating records with no continuing value
- b) making it easier and faster to retrieve information by reducing the overall volume of records, and
- c) reduce the likelihood of accidental disclosure of sensitive or confidential information

You may find it helpful to develop a **transitory records policy**, particularly if you intend to scan paper documents into your electronic medical record system before destroying them. A **Transitory Records Policy** will help your staff to identify transitory records, and use and manage them efficiently.



POLICY CONTENT

You may want to include some or all of the following statements in your policy:

- To determine if a record is a transitory record, consider whether or not it falls into any of the following categories:
 - a) *Temporary information*: Records required for specific activities but having no further value once the activity has been completed.
Examples: phone messages, post-it notes, invitations, some cover sheets
 - b) *Duplicates*: Exact reproductions of a master document. Note that if duplicate records have been annotated or altered in any way, it may have become a new record that should be retained.
Examples: photocopies, documents scanned to the electronic medical record system (lab results, physician consults, etc.)
 - c) *Draft documents and working materials*: Including source materials used in preparation of documents and earlier versions of final documents.
Examples: drafts of reports, working notes or tapes

Be sure that draft documents of the following types of records are no longer required for future accountability and documentation purposes:

- i) legal agreements
- ii) policies, standards, and guidelines
- iii) medical or scientific studies

- Transitory records are identified and destroyed after the actions to which they relate or immediate purposes are completed.
- The destruction of transitory records (e.g., shredding documents scanned to the electronic medical record system) does **not** need to be documented by listing the records, or having a staff member sign off the destruction. This **transitory records policy** provides the authority for the destruction of these records.
- Records containing personal health information that are scanned into the electronic medical record are retained for a minimum of _____ after scanning and before destruction, to ensure that the information has been effectively backed up by the system.
- Where practical, transitory records are maintained separate from non-transitory records if they need to be retained for any length of time.
- All confidential transitory records are kept secure and disposed of using containers or shredders designated for confidential records disposal.



Attachments



HIA definitions

Affiliates: includes all employees, volunteers, students, and persons contracted to provide services for custodians.

Custodian: includes the following:

- Regional Health Authorities (RHAs), Alberta Mental Health Board and Alberta Cancer Board
- Other nursing homes and hospitals not owned by the above
- Community Health Councils and subsidiary health corporations of RHAs, Boards
- Boards, committees, panels, councils or agencies established by any of the above
- Minister and the Department of Health and Wellness
- Regulated health professionals paid through the Alberta Health Care Insurance Plan, including physicians, chiropractors, dental surgeons, dental mechanics, opticians, optometrists, podiatrists and osteopaths
- Licensed pharmacists and pharmacies
- Others as listed in the HIA and the regulations made under it

Custody: Physical possession of the health record or information.

Consent: Agreement by an individual to the disclosure of his/her own health information. To be valid, consent must be provided in writing or electronically and must include:

- an authorization for the custodian to disclose the health information specified in the consent
- the purpose for which the health information may be disclosed
- the identity of the person to whom the health information may be disclosed
- an acknowledgment that the individual providing the consent has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent
- the date the consent is effective and the date, if any, on which the consent expires, and
- a statement that the consent may be revoked at any time by the individual providing it (provided in writing or electronically)

Electronic consent is valid only if the level of authentication is sufficient to identify the individual who is granting the consent or revoking the consent.

Control: The authority to exercise control over or to manage the record or information, including restricting, regulating and administering its use, disclosure and disposition.

Disclosure: Although you may disclose health information to another custodian (within the “controlled arena”), in this document disclosure generally deals with release of information to anyone outside the custodian/affiliate relationship.

Health Information:

Recorded information about individuals. There are three types of health information: (1) diagnostic, treatment and care information, (2) registration information (including billing information), and (3) health services provider information (personal information about the individual who provides health services). The collection, use and disclosure of all three types are regulated by the HIA.

Use: Means the internal use of information (i.e., between a physician and his/her staff)

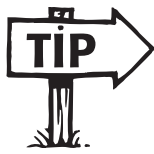
Record: Health information in any form, including notes, images, audiovisual recordings, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner. Does not include software or any mechanism that produces records.

Research: Means academic, applied or scientific health-related research that necessitates the use of individually identifying diagnostic, treatment and care information or individually identifying registration information, or both.



Sample policy statement outline

Following is a standard outline of a policy statement. You can use it as a guide for developing your policy/procedure statements. Feel free to adapt it to make it more appropriate for your practice.



POLICY NAME:

(AND, IT'S A GOOD IDEA TO NUMBER ALL YOUR POLICIES FOR QUICK REFERENCE)

1. Purpose/Rationale

It's helpful to begin a policy/procedure by setting out the purpose or rationale behind it.

For example:

- Legislative requirement to develop a policy, e.g., HIA
- An administrative need to assign responsibilities, e.g., We need to identify who is responsible for _____
- A need to clearly document the steps in a required procedure (how you do things)

2. Scope

Every policy needs a description of scope of the policy. For example, does it apply to:

- all staff, including physicians
- RNs
- administrative personnel
- contractors
- students
- volunteers

What information does it apply to? You may want to state that it applies to all health information, regardless of format. And, you may want to further state that the policy/procedure applies to all facilities and equipment.

You can describe the scope (i) of each policy/procedure you develop or (ii) at the beginning of the group of policies and indicate that it applies to all of them.

3. Policy Description

Policy descriptions set out the privacy positions, or rules that have been adopted or approved in your office. Your policy descriptions may:

- document things you've always done in your practice
- document a new standard to comply with HIA (e.g., the way you handle requests for patient access to medical records)

4. Procedures

Within your policy statement, you may include procedures that apply to the policy. A procedure differs from a policy in that it provides a step-by-step guide to performing a particular action or activity. Ideally, procedures will indicate:

- who is responsible for performing the action
- when the action needs to be performed
- the steps needed to be performed

5. Definitions

It's a good idea to include definitions of any terms used in the policy statement that may be unclear to readers. You can (i) provide definitions at the end of each policy/procedure or (ii) attach a list of definitions to the group of policies and procedures, particularly if terms are used throughout more than one document (see Attachment One for a list of important definitions under HIA).



6. Penalties/Sanctions

Your policy/procedure should include a statement about what happens if the policy is willfully or accidentally breached. For example, penalties/sanctions may include disciplinary action, up to and including dismissal. You may choose to include a general statement about penalties/sanctions early on in your group of policies, rather than repeat the information for each policy.

7. Distribution

Depending on the size of your practice, you may want to print and distribute more than one copy of your policies and procedures. If so, it's a good idea to identify (either at the end of each policy/procedure, or at the beginning of the group of policies) how many copies are in circulation. This is particularly important when it comes time to review and update your policies and procedures – otherwise, you may not recall who has copies, and how many revised copies to print and circulate.

8. Date/Revision Date

It is always a good idea to identify the date of the policy/procedure on the document itself. This is an excellent way to make sure that only the most recent version is available to staff. In order to avoid potential liability issues, you will want to ensure that out-dated policies/procedures are removed from circulation to prevent staff from acting on inaccurate information. Ensuring the original policies/procedures have dates, and indicating the revision dates on any subsequent policies/procedures, will help you to avoid this problem.

9. Approval

You may want to include some space on your policies/procedures for an authorized staff member to sign-off approval of a formally adopted policy/procedure. This will help to distinguish approved, final documents from draft documents.

Attachment three



Request to access health information

(Adapted from *Health Information Act: Guidelines and Practices*, Alberta Health and Wellness, 2001)

The information on this form is collected under Alberta's *Health Information Act* and will be used to respond to your request for your own health information.

<input type="checkbox"/> Mr.	<input type="checkbox"/> Ms	<input type="checkbox"/> Dr.	Last Name	First Name
<input type="checkbox"/> Mrs.	<input type="checkbox"/> Miss			

Mailing Address

City or Town	Province	Postal code
--------------	----------	-------------

Telephone (Business)	Telephone (Home)
----------------------	------------------

Fax number	E-mail Address
------------	----------------

Date of birth (d/m/y)	Other
-----------------------	-------

Provide a description of the information you want to access, in as much detail as possible. Indicate if you also want access to records about the disclosure of your information. *(Be sure to give all your previous names. If you are requesting access to another individual's information, you must include information to identify the individual and attach proof that you can legally act for that individual.)*

Please indicate if you wish to:

Receive a photocopy of the specified record

Please note that a base fee of \$25 applies. For convenience, you may enclose this fee with your request. You should be provided with an estimate of any additional costs.

View the original record, without receiving a copy

Please ask for an estimate of the fee you will pay for:

- review of the original by the physician and/or
- supervision by physician or designated staff person of your review

A deposit of 50% of the fee may be required.

Signature

Date

Section 104 of the *Health Information Act* identifies those individuals who may, on behalf of another individual, exercise the rights and powers conferred on that individual under the Health Information Act. Those situations are listed below. **Please check the box that applies to the right by which you are requesting access to health information**

- if the individual is 18 years of age or older, by the individual
- if the individual is under 18 years of age and understands the nature of the right or power and the consequences of exercising the right or power, by the individual
- if the individual is under 18 years of age but does not meet the criterion in clause (b), by the guardian of the individual,
- if the individual is deceased and was 18 years of age or over immediately before death, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate
- if a guardian or trustee has been appointed for the individual under the Dependent Adults Act, by the guardian or trustee if the exercise of the right or power relates to the powers and duties of the guardian or trustee
- if an agent has been designated under a personal directive under the Personal Directives Act, by the agent if the directive so authorizes,
- if a power of attorney has been granted by the individual, by the attorney if the exercise of the right or power relates to the powers and duties conferred by the power of attorney
- if the individual is a formal patient as defined in the Mental Health Act, by the individual's nearest relative as defined in that Act if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act, or (i) by any person with written authorization

Regulated fee schedule under HIA

Under section 67(1) of the *Health Information Act*, custodians may charge fees for services provided in response to requests to access information. Fees are not charged in respect of a request for access to an applicant's own health information, except for the cost of producing a copy of the record (and then only the amount in excess of \$5.00 is charged).

The following fees are the *maximum* amounts that can be charged to applicants:

- | | |
|--|--------------------------------------|
| 1) Photocopies, hard copy laser print and computer print outs | \$0.25 per page |
| 2) Floppy disks | \$10.00 per disk |
| 3) Computer tapes | \$55.00 per tape |
| 4) Photographs (color or black and white from negative) | |
| a) 4" x 5" | \$10.00 |
| b) 5" x 7" | \$13.00 |
| c) 8" x 10" | \$19.00 |
| d) 11" x 14" | \$26.00 |
| e) 18" x 20" | \$32.00 |
| 5) Radiology film | \$5.00 each |
| 6) Producing a record from an electronic record: | |
| a) computer processing | actual costs |
| b) computer report generation | \$10.00 per 1/4 hour |
| 7) other direct costs: | |
| a) charges to retrieve records or to return past records, or both, from another location | contracted fee or costs average |
| b) courier charges or delivery charges, or both, to send copies to applicant other than by mail or fax | actual costs |
| 8) Severing or supervision: | |
| a) If a physician or specified staff must supervise an in-person review of original documents, or must sever information from records, the regulations also specify amounts that can be charged for that time. These fees include: | |
| • Supervision of applicant's examination of original records | \$6.75 per 1/4 hour |
| • Severing time to determine whether a record requires severing and determining the parts of the record to be severed: | |
| • technician time | \$6.75 per 1/4 hour, maximum 3 hours |
| • health services provider time | \$45 per 1/4 hour, maximum 3 hours |

Request to correct or amend health information

(Adapted from *Health Information Act: Guidelines and Practices*, Alberta Health and Wellness, 2001)

The information on this form is collected under Alberta's *Health Information Act* and will be used to respond to your request for correction or amendment.

<input type="checkbox"/> Mr.	<input type="checkbox"/> Ms	<input type="checkbox"/> Dr.	Last Name	First Name
<input type="checkbox"/> Mrs.	<input type="checkbox"/> Miss			

Mailing Address

City or Town	Province	Postal code
--------------	----------	-------------

Telephone (Business)	Telephone (Home)
----------------------	------------------

Fax number	E-mail Address
------------	----------------

Date of birth (d/m/y)	Other
-----------------------	-------

Whose information do you want to correct?

- your own health information
- another person's health information (*Please include information to identify the other individual and attach proof that you can legally act for that individual.*)

Provide a description of the information you want to correct or amend, in as much detail as possible. (*Be sure to give the complete name that is in the records if it is different from the name given above. If you need more space, please attach a separate sheet of paper.*)

What correction or amendment do you want to make and why? *(Please attach any documents that support your request.)*

Signature

Date

Section 104 of the *Health Information Act* identifies those individuals who may, on behalf of another individual, exercise the rights and powers conferred on that individual under the Health Information Act. Those situations are listed below. **Please check the box that applies to the right by which you are requesting access to health information**

- if the individual is 18 years of age or older, by the individual
- if the individual is under 18 years of age and understands the nature of the right or power and the consequences of exercising the right or power, by the individual
- if the individual is under 18 years of age but does not meet the criterion in clause (b), by the guardian of the individual,
- if the individual is deceased and was 18 years of age or over immediately before death, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate
- if a guardian or trustee has been appointed for the individual under the Dependent Adults Act, by the guardian or trustee if the exercise of the right or power relates to the powers and duties of the guardian or trustee
- if an agent has been designated under a personal directive under the Personal Directives Act, by the agent if the directive so authorizes,
- if a power of attorney has been granted by the individual, by the attorney if the exercise of the right or power relates to the powers and duties conferred by the power of attorney
- if the individual is a formal patient as defined in the Mental Health Act, by the individual's nearest relative as defined in that Act if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act, or (i) by any person with written authorization

Components for an affiliate's oath of confidentiality

(Adapted from *Health Information Act: Guidelines and Practices*, Alberta Health and Wellness, 2001)

- A statement, sworn (or affirmed) by the affiliate, stating that:
 - 1) He/she will uphold to the best of his/her ability his/her duties under the *Health Information Act* and the regulations and the custodian's policies and procedures, and that
 - 2) He/she will not disclose or make known any recorded or non-recorded health information of an individual except as authorized by the act, the regulations and the custodian's policies and procedures
- Space for the city, town, village, etc. where the oath is sworn
- Space for the date and signature of a witness
- (Optional) Place for a Commissioner for Oaths to commission the swearing (of affirming) of the oath

Attachment seven



Sample mini-poster

(from *Health Information Act: Guidelines and Practices*, Alberta Health and Wellness, 2001)

The health information that we are collecting is needed to determine your eligibility for the _____ program, service or benefit (or to provide you with diagnostic, treatment and care services) (or for the training of students) (or for research or statistical purposes) (or for other authorized purpose(s) under section 27 of the *Health Information Act*). It is collected under the authority of the (*Mental Health Act*) (or *Cancer Programs Act*) (or *Hospitals Act*) (or *Nursing Homes Act*) (or *Alberta Health Care Insurance Act*) (and/or section 20(b) of the *Health Information Act* – directly related to and necessary to carry out an authorized purpose under section 27) (or other legal authority). The confidentiality of this health information and your privacy are protected by the provisions of the *Health Information Act* (and any other act that is appropriate to add).

If you have any questions about this collection and use of your health information, please talk to one of the staff (or contact) _____ (position) at _____ (business address) or phone _____ (business phone).

Attachment nine



Section 42 notice to recipient to accompany the disclosure of individually identifying diagnostic, treatment and care information by a custodian

DISCLOSURE WITHOUT THE SUBJECT'S CONSENT

The attached individually identifying diagnostic, treatment and care information of _____
_____ (named individual subject) has been disclosed to _____
_____ (name of recipient) by _____
(name of custodian) on _____ (date), without the consent of the subject, but
authorized under the following provision of the *Health Information Act* (mark the appropriate box):

- | | |
|---|--|
| <input type="checkbox"/> To provide continuing treatment and care to the above individual (s.35(1)(b)) | <input type="checkbox"/> and Privacy Commissioner) to carry out his/her duties (s.35(1)(l)) |
| <input type="checkbox"/> To provide information concerning the presence, location, condition, diagnosis, progress and prognosis of the above individual on the above date and the above individual has not requested otherwise (s.35(1)(c)) (Note – recipient must be a family member or another person with whom the individual is believed to have a close personal relationship) | <input type="checkbox"/> To avert or minimize an imminent danger to the health or safety of any person (s.35.(1)(m)) |
| <input type="checkbox"/> To advise family members of the above individual, or a person with whom the above individual is believed to have a close personal relationship, that the individual has been injured, is ill or has died and the individual has not requested otherwise (s.35(1)(d)) | <input type="checkbox"/> To act in the best interests of the above individual if the individual lacks the mental capacity to provide consent (s.35(1)(n)) |
| <input type="checkbox"/> To provide health services to the above individual who is being detained in a penal or other custodial facility (s.35(1)(e)) | <input type="checkbox"/> To provide necessary health services to a descendant of a deceased individual (s.35(1)(o)) (Note – the recipient must be a descendant or a representative under section 104(1)(c) to (i) and the privacy of the deceased individual must be protected) |
| <input type="checkbox"/> To conduct an audit of the information (s.35(1)(f)) (Note – recipient must enter into an agreement with the custodian about non-disclosure and destruction of the information) | <input type="checkbox"/> To comply with another act or regulation of Alberta or Canada that authorizes or requires the disclosure (s.35(1)(p)) |
| <input type="checkbox"/> To carry out quality assurance activities within the meaning of section 9 of the Alberta Evidence Act (s.35(1)(g)) | <input type="checkbox"/> To transfer records to a successor custodian because the first custodian is ceasing to be a custodian (s.35(1)(q)) |
| <input type="checkbox"/> To provide information for a court proceeding or a proceeding before a quasi-judicial body (s.35(1)(h)) (Note – the custodian must be a party to the proceeding) | <input type="checkbox"/> To enable a health professional body to conduct an investigation, a discipline proceeding, a practice review or an inspection (s.35(4)) (Note – the custodian must comply with other relevant legislation and the health professional body must enter into an agreement with the custodian about non-disclosure and destruction of the information) |
| <input type="checkbox"/> To comply with a subpoena, warrant or court order compelling the production of information or with a rule of court that relates to the production of information (s.35(1)(i)) (Note – the recipient body must have jurisdiction to compel the production of information) | <input type="checkbox"/> To allow for permanent preservation and historical research by the Provincial Archives of Alberta or another archives that is subject to this Act or the Freedom of Information and Protection of Privacy Act (s.38) (Note – the custodian must determine that information has enduring value) |
| <input type="checkbox"/> To investigate an offence involving a life-threatening personal injury to the above individual and the above individual has not requested otherwise (s.35(1)(j)) (Note – the recipient must be a municipal or provincial police service) | <input type="checkbox"/> To enable the Minister of Health and Wellness to carry out his duties (s.40) (Note – the custodian must determine if the disclosure is necessary or desirable) |
| <input type="checkbox"/> To detect or prevent fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of Alberta or Canada (s.35(1)(k)) (Note – the recipient must be another custodian) | _____ |
| <input type="checkbox"/> To enable an officer of the Legislature (e.g., Auditor General, Ombudsman, Chief Electoral Officer, Information | Name and Signature of Custodian (or affiliate) |
| | _____ |
| | Date |

Attachment ten



Consent to the disclosure of individually identifying health information

(Adapted from *Health Information Act: Guidelines and Practices*, Alberta Health and Wellness, 2001)

I, _____ authorize
(the attached) individually identifying

- diagnostic, treatment and care information
- registration information

of myself to be disclosed by _____
(name of custodian), in accordance with section 34 of the Health Information Act to

_____ (name of recipient),

for the following purpose(s)

I understand why I have been asked to disclose my individually identifying information, and am aware of the risks and benefits of consenting, or refusing to consent, to the disclosure of my individually identifying health information.

I understand that, under section 58(2) of the Health Information Act, my express wishes must be considered and I have the right to indicate any portion of my health information that I wish to be kept confidential by my physician and not disclosed to others. I may revoke my consent at any time.

Dated this _____ of _____, _____
(day) (month) (year)

Expiry date (if any) _____ of _____, _____
(day) (month) (year)

Patient or Authorized Representative's Signature

Source of Representative's Authority

Patient or Authorized Representative's Name

Witness Signature*

Witness Name

Section 104 of the *Health Information Act* identifies those individuals who may, on behalf of another individual, exercise the rights and powers conferred on that individual under the Health Information Act. Those situations are listed below. **Please check the box that applies to the right by which you are requesting access to health information**

- if the individual is 18 years of age or older, by the individual
- if the individual is under 18 years of age and understands the nature of the right or power and the consequences of exercising the right or power, by the individual
- if the individual is under 18 years of age but does not meet the criterion in clause (b), by the guardian of the individual,
- if the individual is deceased and was 18 years of age or over immediately before death, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate
- if a guardian or trustee has been appointed for the individual under the Dependent Adults Act, by the guardian or trustee if the exercise of the right or power relates to the powers and duties of the guardian or trustee
- if an agent has been designated under a personal directive under the Personal Directives Act, by the agent if the directive so authorizes,
- if a power of attorney has been granted by the individual, by the attorney if the exercise of the right or power relates to the powers and duties conferred by the power of attorney
- if the individual is a formal patient as defined in the Mental Health Act, by the individual's nearest relative as defined in that Act if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act, or (i) by any person with written authorization

* *HIA does not require a witness for disclosure. As a business practice, you may wish to include a witness if you think extra confirmation of the consent may be required.*



Checklist of components for agreement with Information Manager

(Adapted from *Health Information Act: Guidelines and Practices*, Alberta Health and Wellness, 2001)

This document is intended to be used only as a checklist of components for an agreement with an Information Manager under section 66(2). **It does not constitute a precedent of legal advice.** You and your Information Manager need to determine what provisions should be in the agreement, giving consideration to their relationship and the tasks that the Information Manager will perform. You should seek legal counsel as necessary.

INTRODUCTORY MATTERS

- 1) Names of parties
- 2) Authority to enter agreement – section 66(2) of the *Health Information Act*
- 3) Duration of agreement

SERVICES TO BE PROVIDED

- 4) Description of services to be provided by Information Manager
- 5) Description of health information that is the subject of the agreement
- 6) Financial arrangements – could be attached as a schedule

RESPONSIBILITIES OF INFORMATION MANAGER

- 7) The Information Manager must comply with the *Health Information Act*, the regulations under the act and the terms and conditions of the agreement with respect to the health information disclosed to it by the custodian.
- 8) The Information Manager may use the health information only for the purposes specified in the agreement.
- 9) The Information Manager may disclose the information only for the purposes specified in the agreement.
- 10) The Information Manager must comply with the terms and conditions relating to the type of records storage media, the length of time the information is to be retained and the method of disposition to be used in destroying or archiving the information.
- 11) The Information Manager and his/her employees must only modify the information in accordance with the terms of the agreement.

- 12) The Information Manager must protect the information against such risks as unauthorized access, use, disclosure, destruction, or alteration and limit “access” to the information only to those employees who have a need to know. The Information Manager must comply with the requirements of section 60 of the *Health Information Act* and section 8 of the health information regulation relating to the security of health information.
- 13) The Information Manager must notify the custodian in writing immediately if the Information Manager or his/her employees become aware that any of the conditions set out in the agreement have been breached.
- 14) The recorded information held by the Information Manager is under the custody or control of the custodian for the purposes of the *Health Information Act*.
- 15) Requests by individuals, or their authorized representatives, to access information held by the Information Manager will be directed to and handled by the custodian, but the Information Manager will have a specified role in the retrieval of the requested information for the custodian. (Timelines and costs for retrieval should be indicated and in keeping with the provisions of the act and regulations. The timeline for retrieving the requested information and providing it to the custodian should be relatively short, i.e., four-to-five days to fit within the 30 day timeline in the act.)

INDEMNITY

- 16) The Information Manager must agree to be fully and solely responsible for the actions of his/her employees, agents, consultants and other persons respecting the use or disclosure of the information and for any unauthorized disclosure of the information and for any unauthorized disclosure or use of the information as a result of carrying out the agreement, regardless of the cause (including, but not limited to, negligence, misfeasance, malfeasance, accident or neglect) during the term of the agreement or after the expiration or earlier termination of the agreement.
- 17) The Information Manager must agree to hold the custodian harmless from any third-party claims, demands or actions for which the Information Manager is legally responsible, including those arising out of negligence, willful harm or crimes by the Information Manager or his/her employees or agents.
- 18) The Information Manager must agree to indemnify the custodian for any and all costs or expenses paid or incurred by the custodian as a result of any breach of any term or condition of this agreement or contravention of the act or regulations or arising out of any disclosure by the Information Manager of the health information that is subject to this agreement in any manner contrary to the agreement. Such indemnification will survive the termination of the agreement.
- 19) The custodian is not responsible for any bodily or personal injury or property damage or business losses that may be suffered or sustained by the Information Manager, his/her employees or agents in the performance of the agreement.

TERMINATION

- 20) The agreement may be terminated by either party under certain conditions prior to its completion.
- 21) In the event the agreement is breached and/or health information is disclosed or used in contravention of the terms and conditions of the agreement of the act or regulations, the agreement may be immediately cancelled by the custodian and the Information Manager may be found guilty of an offence under section 107(4) of the act.

GENERAL PROVISIONS

- 22) The agreement may be amended or varied in writing with the mutual agreement of the parties.
- 23) The parties must each designate an individual with responsibility for the agreement, notices and communications (include the contact information for the designated individuals).

EXECUTION

- 24) The agreement must be signed by officers or other officials of the parties who have authority from the parties to sign such an agreement.

Sample research agreement

(Adapted from *Health Information Act: Guidelines and Practices Manual*, Alberta Health and Wellness, 2001)

AGREEMENT BETWEEN

(<Name of Custodian>, hereafter referred to as “the Custodian”)

and

(<Name of Lead Researcher>, hereafter referred to as “the Researcher”)

INTRODUCTION

- 1) The Researcher has applied to the Custodian for disclosure of health information for the research purposes described in the project plan or research proposal – application for disclosure of health information to be used in research including the research purpose(s).
- 2) A description of the Research Project is attached as Schedule B.
- 3) The <Name of Ethics Committee> is satisfied that the Researcher has met the requirements of section 50 of the *Health Information Act*, and has approved the project as of <Date of Approval>.
- 4) The Researcher will/has obtained the consents of the individual subjects prior to disclosure of their health information.
- 5) The Custodian has decided to disclose the health information applied for to the Researcher.
- 6) This Research Agreement applies for the duration of the Research Project, which will begin on <Start Date> and end on approximately <End Date>. The Research Agreement may be extended with approval of the Custodian.

RESPONSIBILITIES OF THE RESEARCHER

- 7) The Researcher agrees to comply with
 - The *Health Information Act* and all regulations made under it.
 - Any conditions imposed by the Custodian relating to the use, protection, disclosure, return or disposal of the health information.

- Any requirements of the Custodian to provide safeguards against the identification, direct or indirect, of an individual who is the subject of the health information.
- 8) The Researcher understands that if he/she knowingly breaches the terms and conditions of the Research Agreement, he/she is guilty of an offence and may be liable to a fine of up to \$50,000.

RESPONSIBILITIES OF THE CUSTODIAN

- 9) The Custodian agrees to disclose the health information or data in a specific format at a specific time(s) (see Schedule C – specifics of the health information and any other information to be disclosed).
- 10) The Custodian agrees to attempt to obtain consents to contact the individuals who are the subject of the information to obtain additional data, if requested by the researcher.

RESTRICTIONS ON USE AND DISCLOSURE OF HEALTH INFORMATION

- 11) The Researcher agrees to only use the research information for purposes identified in Schedule A.
- 12) The Researcher agrees not to use or disclose the information for any subsequent or other purposes not identified in Schedule A without the prior written approval of the Custodian, and/or the consent of the individual who is the subject of the information, if required by the Custodian.
- 13) The Researcher agrees to disclose information only to individuals with a need to know who are working with the Researcher on the Research Project (include names of individuals).
- 14) The Researcher agrees to ensure that all individuals on the research team that have access to the health information comply with the *Health Information Act* and regulations and with any conditions imposed by the Custodian.

PUBLICATION OF RESULTS

- 15) The Researcher agrees that no identifying information or information that could be manipulated to identify an individual will be published.
- 16) The Researcher agrees to provide the Custodian with the proposed report (or publication) of the results of the research for the Custodian's review and the Custodian agrees to acknowledge its receipt. The report (or publication) must include a statement that some of the information used in the study was provided by the Custodian and the Custodian expresses no opinion on the interpretations and conclusions in the publication.

REQUIREMENTS TO SAFEGUARD DATA

- 17) The Researcher agrees to adequately safeguard the confidentiality and security of the health information obtained from the Custodian. The Researcher also agrees to safeguard the privacy of the individuals who are the subjects of the information by ensuring that the individuals who are the subjects of the information cannot be identified, directly or indirectly.

- 18) The Researcher agrees to report to the Custodian any breaches of confidentiality and/or security respecting the information and to take steps to both remedy the breach and prevent similar occurrences in the future.
- 19) The Researcher agrees to allow the Custodian to access or inspect the Researcher's premises to confirm that the Researcher is complying with the act and regulations, any imposed conditions on use, protection, disclosure, return or disposal of the information and any requirements related to the provision of security safeguards.
- 20) The Researcher agrees to dispose of the information by <Date of Disposal> after the research has been completed by <Method of Destruction>, or by returning it to the Custodian by <Date of Return>.

FINANCIAL ARRANGEMENTS

- 21) The Researcher agrees to pay the Custodian the amount of <Fees>, to cover the cost of preparing information, transmission, photocopying, obtaining consents, etc.

TERMINATION

- 22) In the event the agreement is breached and/or health information is disclosed or used in contravention of the terms and conditions of the agreement or the act or the regulations, the agreement may be immediately cancelled by the Custodian, the research privileges of the Researcher may be withdrawn, all research information may need to be returned to the Custodian and the Researcher may be found guilty of an offence under section 107 of the act.
- 23) The agreement may be terminated by either party under certain conditions prior to its completion.

INDEMNITY

- 24) The Researcher agrees to hold the Custodian harmless from any third-party claims, demands or actions for which the Researcher is legally responsible, including those arising out of negligence, willful harm or crimes by the Researcher.
- 25) The Researcher agrees to indemnify the Custodian for any and all costs or expenses paid or incurred by the Custodian as a result of any breach of any term or condition of this agreement or contravention of the act or a regulation under the act or arising out of any unauthorized disclosure by the Researcher of the health information that is subject to this agreement in any manner contrary to the agreement. Such indemnification will survive the termination of the agreement.
- 26) The Custodian is not responsible for any bodily or personal injury or property damage or business losses that may be suffered or sustained by the Researcher, or any other member of the research team.
- 27) The Researcher has no recourse against the Custodian for any loss or damage arising from any advice provided by the custodian about the research information.

TERMINATION OF AGREEMENT

- 28) This agreement may be terminated by either party at any time subject to the following conditions (state the conditions for termination by Custodian or Researcher, and address the retention, disposition or return of health information).
- 29) The Researcher agrees that the consent of the Custodian has been obtained prior to the transfer of the agreement to another person. Consent may be arbitrarily withheld at the discretion of the Custodian. Successors must be bound by the terms and conditions of the agreement.

Signature of Researcher

Printed Name of Researcher

Signature of Custodian Representative

Printed Name of Custodian Representative

Date of Agreement