Department of Medicine

Health Information Privacy and Security Policy and Procedures

Table of Contents

Health Information Privacy and Security Policy

Overview

The collection, use and disclosure of health information by custodians and their affiliates are governed by the Health Information Act (HIA) and this policy. The principles and the procedures appended to this policy are intended to enable patient care and effective service delivery, while ensuring the privacy of patients.

Scope

This policy applies to:

- All faculty, learners, staff, and third party contractors who need to access health information that is in the custody and/or control of physicians in the Department of Medicine;
- health records in any form, created or received in the course of carrying out health services, education and/or research;
- all facilities and equipment required to collect, manipulate, transport, transmit or keep health information.

Policy Statement

In accordance with the HIA, all physicians, staff and learners (fellows, residents, students) shall protect the confidentiality of health information in their custody or control, and the privacy of the individuals who are the subjects of that information. This includes protection against unauthorized use, disclosure, modification, or access to the information.

Physicians, who are custodians of health information, and their affiliates, are expected to comply with the HIA, this policy and associated procedures with respect to health services provided to their patients. All records related to a health service shall be deemed to be under the custody and control of the physician who provided the service.

Failure to comply with this policy and its procedures may place an individual at risk of prosecution under the HIA.

Information Handling and Security Procedure

Overview

The information security provisions of the Health Information Act (HIA) require custodians to protect health information in their custody or control by making reasonable security arrangements to protect against unauthorized access, collection, use, disclosure or destruction. The Act also requires custodians to take appropriate safeguards for the security and confidentiality of records, including addressing the risks associated with electronic health records. This procedure outlines administrative, technical and physical safeguards to protect health information.

This procedure recognizes that faculty, learners, and staff work in integrated environments that may be governed by Alberta Health Services (AHS), University of Alberta, and/or private corporations.

This procedure sets out the minimum standards for handling health information.

Procedure

1. Administrative Safeguards

1.1 The need for confidentiality and security of information shall be addressed as part of the conditions of employment for all staff by having the individual review and sign a confidentiality agreement. Within educational programs, learners are expected to complete the Professional Standard for Students Form (http://education.med.ualberta.ca/admin/policies/standard/Pages/default.aspx).

1.2 The least amount of information necessary for the intended purpose will be used or disclosed, and only to affiliates or recipients with a need to know. If the intended purpose can be accomplished without use or disclosure of identifying information, then the information shall be made anonymous.

1.3 Health information is not transmitted if conversations can be overheard; or if other methods of communication can be intercepted (e.g., text messages).

1.4 When working in a clinical setting, patients and visitors are accompanied by a staff member to private or semi-private areas such as examination rooms or offices.

1.5 Faculty and staff who are accessing and using health information are expected to complete HIA awareness training. The following training options are available:

- AHS online privacy and security training: http://www.albertahealthservices.ca/3962.asp. This module provides HIA awareness as well as training on AHS security and privacy policies. This online training course is recommended for any University faculty member or staff who has a dual role with AHS.
- AHS HIA Awareness training: face to face course. This module provides basic HIA awareness training for eCLINICIAN end users only.
- FoMD online privacy training: https://moodle.med.ualberta.ca/course/view.php?id=117. This module provides basic HIA awareness training and is available to any member of the FoMD. This online training course is recommended for any University faculty member or staff who works entirely in the context of the University of Alberta (no formal role with AHS).

1.6 Faculty and staff are expected to complete HIA awareness training on a yearly basis. Managers are responsible for maintaining HIA awareness certificates of completion in the personnel file for

support staff. Faculty (physician and non-physician) are responsible for maintaining their own records of HIA awareness training completion.

1.7 As stipulated in the HIA, before implementing new administrative practices or information systems related to the collection, use and disclosure of health information, custodians shall complete a privacy impact assessment (PIA) for submission to the Office of the Information and Privacy Commissioner (OIPC). The PIA will describe how the new initiative will affect privacy, and what measures the custodian will put in place to mitigate risks to privacy. More information about PIAs requirements can be found on the OIPC website: http://www.oipc.ab.ca/pages/PIAs/PIARequirements.aspx.

1.8 Individuals shall report any violations or breaches of information security as soon as possible to their manager (e.g. immediate supervisor, director, assistant chair) or department chair so that corrective action can be taken to resolve the immediate problem and minimize the risk of future occurrence.

1.9 Health information is retained in accordance with the records retention provisions outlined by the appropriate health professional regulatory body (e.g., College of Physicians and Surgeons of Alberta Standards of Practice).

1.10 Information handling obligations are clearly defined by contracts with information managers, contractors, and other external recipients.

2. Technical Safeguards

2.1 When using a Faculty of Medicine & Dentistry (FoMD) and/or AHS managed computer, each individual must have a unique user id and password.

2.2 When using a non-managed computer (e.g. personal or home computer), each individual must ensure they have installed (and updated) antivirus and antispyware (i.e. anti-malware) software that runs automatically.

2.3 Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff.

2.4 Computers must default to a screensaver or be locked after a maximum of 15 minutes of inactivity or such lesser period of time as does not affect the efficiency of operations, and require password entry to reactivate. All computers must be logged off at the end of the business day.

2.5 Health information will not be sent via e-mail over public or external networks without the use of appropriate security measures such as encryption or virtual private network.

2.6 Health information must be protected as per the Faculty of Medicine & Dentistry's Encryption Policy and Faculty of Medicine & Dentistry USB Device Usage Policy.

2.7 When using AHS managed computer, health information must be protected as per AHS corporate policies, procedures, and directives (see AHS Insite: http://insite.albertahealthservices.ca/corporate-policies.asp).

3. Physical Safeguards

3.1 All records, both on and off site, will be held and stored in an organized, safe and secure manner. Any paper records will be housed in a locked room or in locked cabinets inaccessible to the public.

3.2 Clinical areas and staff offices that are not in an Alberta Health Services facility must have fire protection and suppression systems in place. At a minimum this includes smoke detectors and a fire extinguisher.

3.3 Managers must ensure that there are controls in place over who has keys, access cards or access codes to areas where health information or computers are housed. Keys or door access codes should only be assigned to those who need them for their job function and must be returned to the designated administrative personnel on termination of employment or contract. A security assessment must be conducted to determine if locks must be changed if keys are not returned or it is suspected that copies have been made.

3.4 Buildings or areas that contain health information or computer equipment must be protected by security measures.

3.5 Health information will not be displayed or left unattended in public areas.

3.6 Health information that is transported will be sealed, marked as confidential, and directed to the attention of the authorized recipient.

3.7 Staff will verify the credentials and identity of courier services used to transport health information.

3.8 All fax transmissions will be sent with a cover sheet that indicates the information being sent is confidential and giving a telephone number to call if received in error. Fax transmissions may be sent directly from an electronic medical record system. In such cases, numbers will be verified before being entered into the fax directory. Reasonable steps will be made to confirm that confidential information transmitted via fax is sent to a recipient with a secure fax machine and that fax numbers are confirmed before information is transmitted. Fax machines that are used to receive health information should be placed in a secure location with limited access or fax transmissions should be routed electronically to a MedIT or AHS file server.

3.9 All computer equipment will be physically secured to standards set by AHS and/or FoMD MedIT. Portable computers, tablets, smart phones shall be locked up when not in the physical possession of a user.

3.10 Information that is not confidential or sensitive in nature will be disposed of by placing it in recycling bins. All records containing identifiable health information will be destroyed by shredding or placed in approved shredding bins (ex: Shred-it).

3.11 Removal of University computer equipment will be conducted in accordance with the University's Equipment and Furnishings Asset Management Policy.

4 Transitory Records

Transitory records are documents that are required for routine or short term transactions, and contain little or no information of ongoing legal or business value. They should be identified and destroyed (where possible) as soon as they have fulfilled their purpose.

4.1 Types of transitory records that are relevant to this procedure:

- Temporary information, such as phone messages, voice mails, post-it notes, invitations and cover sheets.
- Duplicates – exact copies of records maintained as master copies and that have not been altered or added to in any way. Includes photocopies, electronic copies of faxes,

paper or voice records that are scanned to a file server and/or information system, dictated audio records that have been transcribed.

- Draft documents, including source materials used in preparation of documents, draft reports, earlier versions of completed documents.

4.2 Records containing health information that are scanned into an electronic medical record system will be retained for a minimum of 1 week after scanning and before destruction, to ensure that the information has been effectively backed up by the system. Adequate quality assurance processes must be in place before scanned documents can be shredded (e.g., for new staff, 100% review of all scanned documents, then scaling down to as little as 2% if the scanning process is proving to be error-free).

4.3 Where practical, transitory records are kept separate from records retained for business or legal purposes while in use.

4.4 Transitory records containing health information will be shredded in accordance with section 4.1 above.

Collection, Use and Disclosure of Health Information Procedure

Overview

The Health Information Act (HIA) provides rules for the collection, use and disclosure of identifying health information. Custodians of health information are bound by these rules and this procedure provides guidance for their application.

Further information about processing requests and documenting consent, including sample letters and forms, can be found by referring to the Alberta Health publication: Health Information Act Guidelines and Practices.

Procedure:

1. General Rules

1.1. Individually identifying health information will not be collected, used or disclosed if aggregate or other non-identifying health information is adequate for the intended purpose.

1.2. Individuals will collect, use or disclose the least amount of health information that is necessary to carry out their work activities.

1.3. Before using or disclosing health information, individuals will make a reasonable effort to ensure that the information is accurate and complete.

1.4. Individuals will not use identifying health information to market any service for a commercial purpose or to solicit money without the express consent of the individual who is the subject of that information.

1.5. Individuals, who participate in AHS shared electronic medical records (EMRs), such as eCLINICIAN, will adhere to Collection, Access, Use, and Disclosure policies and procedures that have been developed by the Information Stewardship Office (ISO).

2. Collection and Use of Identifying Health Information

2.1. Health information will be collected directly from the patient, who is the subject of that information, or an authorized representative, unless indirect collection is authorized by HIA. Examples of indirect collection are:

- When the patient authorizes collection from a third party. This authorization can be verbal, however, it should be documented and, whenever possible, the custodian should send a letter to the individual concerned setting out what he or she has authorized. .
- When direct collection would compromise the interests of the patient, the purpose of collection, the accuracy of the information or the safety of another person (e.g. patient is not being completely truthful or cannot remember information).
- When direct collection is not reasonably practicable (e.g. language barrier, or cognitive impairment).
- When information is collected from another custodian during referral or consultative processes.

2.2. When collecting health information directly from a patient, the patient will be informed of the purpose for which the information is collected, the legal authority for the collection and the title and business contact information of a staff member who can answer questions. Notification will be done by means of posters in the clinic reception area and/or examination rooms, and verbally when appropriate.

2.3. Health information shall only be used to:

- Provide health services
- Determine or verify the eligibility of the individual to receive a health service
- Education of health service providers
- Carry out purposes authorized by federal or provincial legislation (e.g. *Public Health Act*)
- Obtain or process payment for health services
- Internal management purposes, including quality improvement and monitoring processes,
- Conducting research into better health practices, services or management (under specific conditions, for example, researchers must have research ethics board approval before using health information),
- or for other purposes set out in section 27 of HIA.

2.4. Health Information shall only be used by individuals as required to perform their assigned duties.

3. Disclosure with Consent

3.1. Individuals will obtain written or electronic consent from a patient to disclose identifying health information to anyone other than the patient, their authorized representative, or to another custodian.

3.2. Consent must adhere to requirements set out in section 34(2) of HIA.

3.3. Physicians, who are custodians, may seek consent from patients at the time of referral, or during a subsequent consultation, to disclose registration information to researchers. This will enable a researcher to contact individuals to determine if they are interested in participating in a research project.

4. Disclosure without Consent

4.1. Custodians may, but are under no obligation to, disclose identifying health information without consent in the following circumstances:

- As per sections 35-40, and 46-47 of HIA.
- To another custodian, or affiliate of a custodian, for the legally authorized uses identified in section 27 of HIA.
- To a researcher (subject to health research ethics board review and approval), who has signed a written research agreement with the custodian in accordance with HIA.

4.2. In all cases, custodians must consider the expressed wishes of the patient with regard to his or her health information and disclose the least amount of identifying health information at the highest level of anonymity that they consider necessary to fulfill the request.

5. Notation and Notification

5.1. When a record containing health information is disclosed the custodian or authorized affiliate will make note of the following information and place it on the patient's medical record:

- The name of the person to whom the information is disclosed;
- The date and purpose of the disclosure, and;
- A description of the information disclosed.

5.2. When disclosure is from one custodian to another custodian, and the disclosure is authorized through an electronic medical record system (EMR), the audit trail of the EMR is deemed to be sufficient record of the disclosure.

Right of Access to Health Information Procedure

Overview

Subject to limited and specific exceptions in the Health Information Act (HIA), individuals have a right of access to information about themselves that is in the custody or control of a regulated health professional (e.g., physician, dentist, pharmacist) and the right to request corrections or amendments to this information.

This procedure is intended to define a process for facilitating requests for access to and correction of an individual's own health information.

Further information about processing requests, including model letters, forms, and guidance on applying exceptions can be found by referring to the Alberta Health publication: Health Information Act Guidelines and Practices.

Procedure

1. General Procedures

1.1. During the provision of health services, custodians (i.e. physicians) and their affiliates (i.e. support staff and learners) will share information verbally with the patient or authorized representative and allow access to or provide copies of their health information records when practical.

1.2. In the case of a request by the parent or guardian of a minor, the custodian will determine whether the minor understands the consequences of disclosing or not disclosing the health information before making a decision to share information with the parent or guardian.

1.3. When an individual or authorized representative asks for a correction of factual information and can substantiate that the information is incorrect, an authorized individual (custodian or affiliate) will make the correction to the medical record. (Examples include name, address, telephone number and other demographic information).

1.4. Requests for information contained in an AHS shared EMR (e.g., eCLINICIAN) will be referred to the Information Stewardship Office for processing.

2. Procedure to Request Access to Information

2.1. When access cannot be provided under section 1.1 of this procedure, patients may make a request for access to information in writing. An individual may request access to another person's information only if they are an authorized representative.

2.2. Requests for access to information that are not covered in section 1.4 of this procedure should be directed to the physician who provided care and is the custodian of the patient's health information.

2.3. After receiving the request, the custodian (or his/her affiliate) will ensure the retrieval of the requested records and, in accordance with the fee schedules set out in the Health Information Regulation, prepare a fee estimate and provide that estimate to the applicant. The applicant has up to 30 days to indicate if the fee estimate is accepted or to modify the request to change the amount of fees assessed.

2.4. 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 or on the receipt of at least 50% of any estimated fee.

2.5. Custodians may agree to waive fees, including the basic fee, for reasons of financial hardship or fairness.

2.6. Once the estimate has been agreed to, the custodian will review the records subject to the access request for possible exceptions to disclosure and ensure that copies are prepared for disclosure. All records relating to the request will be reviewed on a line-by-line basis.

2.7. Response to the applicant must be made within 30 days of receipt of the request unless the time limit has been extended in accordance with HIA.

2.8. As part of the response, the applicant shall be told:
- Whether access to the record or partial record is granted or refused;
- If access is granted, where, when and how access will be given, and
- If access is refused, the reasons for refusal and basis of refusal; the name, title, business address and phone number of the health professional; and that the applicant has a right to request a review of the decision by the Alberta Information and Privacy Commissioner.

2.9. The custodian or his/her affiliate 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 original record.

3. Authentication of Recipient

3.1. When an authorized representative requests an individual's health information, a custodian (or his/her affiliate) may request documentation of the representative's authority to act and verify that the powers and duties of the representative allow for requesting health information on behalf of the individual. If the authorized representative is not known to the custodian or affiliate, a copy of such documents as a guardianship order, power of attorney, personal directive or letters of administration for an estate must be shown.

3.2. Custodians and affiliates shall take reasonable steps to verify the identity of the individual or authorized representative before disclosing health information. This may involve looking at a driver's license or health card.

4. Right to Refuse Access to Health Information

4.1. Custodians **must refuse** to disclose health information to an applicant:
- If it is about an individual other than the applicant;
- If it sets out procedures or contains results of an investigation, discipline proceeding, practice review or inspection relating to a health services provider; or
- If disclosure is prohibited by provincial legislation (e.g. information protected under the *Protection for Persons in Care Act*, information about organ or tissue donations).

4.2. Custodians have the **discretion to refuse** disclosure of health information to an individual:
- If it could cause harm or cause mental distress to the subject or another individual;
- If it poses a threat to public safety;
- If it could reasonably lead to the identification of a person who provided health information in confidence and the physician considers it to be appropriate that the name of the person be kept confidential;
- If it could prejudice the use or results of audits, diagnostic tests or assessments.

4.3. Records may contain both information that can be released and other information that, for reasons listed above, should be excluded from a disclosure to an applicant. In this case, the custodian may choose to sever the records. Custodians and their affiliates should review the Alberta Health, Health Information Act Guidelines and Practices for complete details regarding procedures for severing records.

5. Procedure to Request Correction of Health Information

5.1. When information cannot be corrected under section 1.3 or 1.4 of this procedure, an individual (or their authorized representative) may make a request for correction or amendment in writing. An individual may request a correction to another person's information only if they have written authorization of the individual the information is about.

5.2. The custodian will review the request to determine whether the request is to be granted or refused. Corrections will only be made to factual information. Corrections cannot be made to professional opinions or observations. The correction process must be completed within 30 days of receipt of the request for correction, unless the time has been extended under HIA.

5.3. When a custodian determines that a correction or amendment is to be made, the custodian must ensure that the correction is made on all records containing the corrected information, and inform the applicant in writing of the corrections made.

5.4. When a custodian refuses to correct or amend the information, they will advise the individual that they may

- Ask for a review of this decision by the Information and Privacy Commissioner, or;
- 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 custodian's decision.

5.5. When the applicant submits a statement of disagreement, the custodian will ensure that the statement is incorporated into the patient's medical record with an appropriate linkage to the information that was not corrected.

5.6. Custodians are responsible for advising persons to whom the information was disclosed in the preceding year if a correction is made to the record.

Health Research Information Management Procedure

Overview

The Health Information Act (HIA) sets out rules for the disclosure of health information for research purposes. These rules are in sections 48 – 56 of the Act.

For the purpose of this procedure, the term "researcher" means a principle investigator (or co-investigators, if multiple researchers share primary responsibility for the research) conducting research that necessitates the use of health information. Research staff and students are considered "research affiliates". Researchers and research affiliates are all responsible for adhering to the HIA and this procedure.

This procedure sets out guidelines for the following clinical research scenarios:

- **Collection of health information by a Faculty member, who is a researcher, from a custodian:** Faculty member requests access to patient records from a custodian. The custodian of the records might be AHS, Covenant Health, a physician in the community, or a colleague within the Faculty. Faculty members should keep in mind that AHS and/or Covenant Health are typically the custodians of patient records within their facilities, as governed by the Hospital Act (e.g., Emergency Department, Intensive Care Unit, Inpatient Ward, most outpatient clinics that are program based).
- **Collection and use of health information by a Faculty member, who is a custodian, for his/her own research purposes**. Faculty member, who is a custodian, uses patient records that are in his/her custody and control for his/her own research purposes.
- **Disclosure of health information by a Faculty member, who is a custodian, to a researcher**: Faculty member, who is a custodian, provides health information or patient records that are in his/her custody and control to another Faculty member, or an external researcher, for research purposes.

Procedure

1. Collection of Health Information for Research by a Researcher

1.1. Before collecting health information for research purposes, researchers shall obtain approval from the Health Research Ethics Board.

1.2. Researchers shall submit a written application to all custodians in order to request disclosure of health information to be used in research. Applications may vary depending on the custodian's requirements, but should include the following at a minimum:

- a copy of the research proposal
- a copy of the Ethics Board's response to the research proposal
- summary of health information that is to be used in the research project.

1.3. If the custodian(s) agree to disclose the requested health information, the researcher shall sign a research agreement that complies with section 54 of HIA.

1.4. All research requests for health information in an AHS Shared EMR (e.g., eCLINICIAN) will be submitted to the Information Stewardship Office.

2. Collection and Use of Health Information for Research by a Custodian

2.1. Before using health information from health records in his/her own custody for research purposes, a custodian must determine whether the research purposes can be achieved without using identifying health information. If so, the custodian must strip, encode or otherwise transform the individually identifying health information to create non-identifying health information. If it is not possible to achieve the research purposes with non-identifying health information, the custodian must submit a research proposal to the Health Research Ethics Board and include with that proposal the consent form that will be used to obtain individual consent or the rationale for not requiring such consent. The custodian must receive the committee's approval letter prior to commencing research.

3. Disclosure of Health Information for Research by a Custodian

3.1. If an individual has consented in the prescribed manner to having his/her registration information disclosed for the purpose of determining participation in a research project, or if consent has been waived by the Health Research Ethics Board; the custodian may disclose that information to a researcher when the custodian believes that participation in the research project is in the patient's interests.

3.2. Upon receipt of a request for disclosure, a custodian may, but is not required to, disclose the health information applied for. If the custodian decides to disclose the health information, he or she may impose any conditions on the researcher that he or she feels necessary in addition to any conditions imposed by the Health Research Ethics Board.

3.3. If consents are required from the individuals whose health information is being disclosed, custodians must verify that consent has been obtained either by seeing the consent forms from a random sample or from the full study population.

3.4. Custodians may assign costs associated with preparing the records for disclosure, copying health information and obtaining consent. Such costs must not exceed the actual cost of the work.

4. Research Agreements

4.1. In compliance with section 54 of the HIA, a research agreement must be entered into between the custodian and the researcher in which the researcher agrees to:

- comply with the Health Information Act and regulations;
- comply with any conditions imposed by the custodian relating to the use, protection, disclosure, return or disposal of the health information;
- comply with any requirement imposed by the custodian to provide safeguards against the identification, direct or indirect, of an individual who is the subject of the health information;
- use the health information only for the purpose of conducting the proposed research;
- not to publish the health information in a form that could reasonably enable the identity of individuals to be readily ascertained;
- only contact individuals to obtain additional health information if the individuals consent to being contacted;
- allow the custodian to access or inspect the researcher's premises to ensure that researcher is complying with the terms of the agreement, and
- to pay any costs related to preparing the records for disclosure, copying the health information or obtaining consents for further contact of individuals.

5. Protection of Health Research Information

5.1. Health information that is collected by researchers and/or research affiliates must be protected using the administrative, technical, and physical safeguards outlined in the Information Handling and Security Procedure above.

Definitions

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use.

Affiliates	Includes all employees, volunteers, students, residents, fellows and persons contracted to provide services for custodians.
Authorized Representative	Means any person who can exercise the rights or powers conferred on an individual under applicable privacy legislation. This includes the right of access to an individual's health information and the power to provide consent for disclosure of such information. • If the individual is under 18 years of age, and does not understand the nature of the right or power or the consequences of exercising the right or power, by the guardian of the individual; • If the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the estate; • A guardian or trustee appointed under the Dependent Adults Act if the right or power related to the powers or duties of the guardian or trustee; • An agent under the Personal Directives Act if the directive so authorizes; • A person who has power of attorney granted by the individual if the exercise of the right or power relates to the powers or 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 the Act if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that Act. • Any person with written authorization from the individual to act on the individual's behalf.
Consent	Agreement by an individual to the disclosure of their own health information to a third party. The consent must include: • An authorization for the custodian to disclose the information specified in the consent • The purpose for which the information may be disclosed • The identity of the person to whom the information may be disclosed • An acknowledgement that the individual providing the consent has been made aware of the reasons why the 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 • A statement that the consent may be revoked at any time by the individual providing it. A consent or revocation of consent can be 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. In the case of a minor who has consented for diagnosis or health services, consent for the release of information must be obtained from the minor (not the parent or guardian).
Custodian	Includes health service providers who receive and use health information and are responsible for ensuring that it is protected, used, and disclosed appropriately. In the context of the Faculty of Medicine and Dentistry, custodians may include: • regulated members of the College of Physicians and Surgeons of Alberta • regulated members of the College of Alberta Denturists; • regulated members of the Alberta Dental Association and College; • regulated members of the College of Registered Dental Hygienists of Alberta; • regulated members of the Alberta College of Pharmacists; • Alberta Health Services; • Covenant Health. Please note this is not an exhaustive list. For full list of custodians, please refer to definitions in the HIA.
Data Matching	Means the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from two or more electronic databases, without the consent of the individual.
Diagnostic, treatment and care information	Includes information about the following: • the physical and mental health of an individual; • a health service provided to an individual • information about the health service provider who provided a health service to an individual • donation by an individual of a body part or substance, including information derived from the testing or examination of a body part or bodily substance; • a drug as defined in the *Pharmacy and Drug Act* provided to an individual; • a health care aid, device, product, equipment or other item provided to an individual pursuant to a prescription or other authorization; • the amount of any benefit paid or payable under the *Alberta Health Care Insurance Act* or any other amount paid or payable in respect of a health service provided to an individual; • any other information about an individual that is collected when a health service is provided to the individual but does not include information that is not written, photographed, recorded or stored in some manner in a record.

Disclosure	Means the release, transmittal, exposure, revealing, showing, providing copies of, telling the contents of, or giving health information by any means to any person or organization. It includes disclosure to another custodian or to a non-custodian. A custodian making health information accessible to other custodians via the Alberta electronic health record does not constitute a "disclosure".
Health Information	Information that identifies an individual and is stored in any format that relates to: diagnosis, treatment and care; registration information (e.g. demographics, residency, health services eligibility, or billing).
Information Stewardship Office (ISO)	Office established in order to oversee all activities relating to the confidentiality and privacy of information in AHS Shared electronic medical record systems that governed by the *Provincial Information Sharing Framework Agreement*. Faculty members, who are physicians and are participating in AHS Shared electronic medical record systems, will be governed by this agreement and subject to policies and procedures developed by the Information Stewardship Office.
Non-identifying health information	Information in which the identity of an individual cannot be readily ascertained.
Registration Information	Includes information relating to an individual that falls within the following general categories: • Demographic information, including the individual's personal health number • Location information • Telecommunications information • Residency information • Health services eligibility information • Billing information
Research Affiliate	Individuals who conduct research in collaboration with a researcher (other Faculty members, students, staff, contractors, volunteers, etc…).
Researcher	Principal investigator (or co-investigators) involved in clinical research of any kind that necessitates the use of individually identifying diagnostic, treatment and care information or individually identifying registration information, or both.
Manager	Individual with supervisory and/or administrative responsibilities, this may include: • Administrative Professional Officer, Research/Trust Administrators, or designated administrative position (supervising support staff). • Division Director, Director of a Centre or Institute, Department Chair, or other related position (supervising Faculty members).

	• Faculty members themselves, in conjunction with the Associate Deans of Undergraduate and Postgraduate Medicine, (supervising learners). • Researchers (supervising research affiliates).
Use	Means applying health information for a purpose and includes reproducing the information, but does not include disclosing the information.

Related Links

Health Information Act

Health Information Act Designation Regulation

Health Information Act Alberta Electronic Health Record Regulation

Health Information Act Guidelines and Practices (Alberta Health)

Information Stewardship Office (link not available at this time)

Use and Disclosure of Health Information for Research (OIPC)

Related Policies and Procedures

Faculty of Medicine & Dentistry USB Device Usage Policy

Faculty of Medicine & Dentistry Encryption Policy

UAPPOL Information Management & Information Technology Policies

UAPPOL Equipment and Furnishings Asset Management Policy