Original Approval Date: August 1, 2017 | **Most Recent Approval Date: February 22, 2021**

Most Recent Editorial Date: May 15, 2020 | **Next Review Date: February 22, 2024**

Parent Policy: Health Information Privacy and Security Policy

Information Handling and Security Procedure

Office of Administrative Responsibility:	Dean's Office, Faculty of Medicine & Dentistry
Approver:	Dean's Executive Committee, Faculty of Medicine & Dentistry
Scope:	Compliance with this Faculty policy extends to all members of the Faculty of Medicine & Dentistry

Overview

The *Health Information Act* of Alberta (HIA) requires 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 HIA also requires Custodians to implement 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 within the Faculty of Medicine & Dentistry (FoMD).

Procedure

1. Administrative Safeguards

1.1 The least amount of information necessary for the intended purpose will be collected, used and disclosed. Use and disclosure of Health Information will be done on a need to know basis. If the intended purpose can be accomplished without use or disclosure of identifying information, then non-identifying health information shall be used or disclosed instead.

1.2 Identifiable Health Information will be stored, processed, or transmitted in a secure manner.

1.3 Faculty and staff must complete appropriate University and FoMD privacy and security training, refreshed periodically as appropriate, according to this section:

- Faculty and staff who use University information management services must, before handling any personal information, complete the University Security & Privacy Education Declaration (SPED) training, and must complete the corresponding Acknowledgment of Privacy and Security Obligations annually.
- Faculty and staff who have a dual role with AHS or Covenant Health and use AHS information management services (e.g. AHS managed clinical information systems such as Connect Care), will be required to follow the relevant AHS policies and procedures associated with access to such systems. must complete any required AHS privacy & security training.
- FoMD Custodians and their Affiliates must, before handling any Health Information, complete the FoMD online HIA training course, and obtain a Certificate of Achievement by passing the Quiz, and retake the course every 3 years.

University of Alberta supervisors will be responsible for ensuring support staff have completed the online HIA training according to this section, and for maintaining up to date Certificates of Achievement. Faculty members will otherwise be responsible for ensuring themselves, and any individuals directly hired by those Faculty members, have completed the online HIA training according to this section, and for maintaining up to date Certificates of Achievement.

1.4 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 of Alberta (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. Existing PIAs submitted on behalf of the FoMD or a Department may be applicable or amended when appropriate. More information regarding PIA requirements can be found on the OIPC website: https://www.oipc.ab.ca/action-items/privacy-impact-assessments.aspx.

1.5 Faculty and staff must report any actual or suspected privacy and/or security Breach as soon as reasonably possible to:

- Their manager (e.g. immediate supervisor, director, Assistant Chair, etc.);
- MedIT, if the Breach involves the compromise of an information technology resource; and
- The FoMD Health Information Privacy Advisor or Information & Privacy Office.

1.6 As of August 31, 2018, Custodians have a duty to provide notification of a Breach of Health Information to:

- The Office of the Privacy Commissioner of Alberta;
- The Minister of Health; and
- The affected individual,

where the Breach gives rise to a risk of harm to the affected individual. Contact the Health Information Privacy Advisor for advice on what constitutes a Breach, and whether a Breach gives rise to a risk of harm under the HIA. More information is contained in section 4 below.

1.7 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 and the Alberta Dental Association and College) or as required by other organizations such as AHS. Other records management resources include the FoMD Records Retention & Disposition Schedule, University Research Records Stewardship Guidance Procedures and Guidelines, and the University Records Officer.

1.8 Information handling obligations shall be clearly defined by contracts with information managers, contractors, and other external recipients. When contracting with contractors who will have access to personal information that is collected in the course of an operating program or activity of the University, the contract must be reviewed by the Information & Privacy Office as per University policy. Where a third party, such as the University, cloud service provider or otherwise, will provide information manager services as defined in the HIA, the Custodian must enter into an Information Manager Agreement (IMA) with that information manager. For assistance in determining whether an IMA is required, and what an IMA must contain, contact the Health Information Privacy Advisor.

2 Technical Safeguards

2.1 Staff shall ensure that appropriate safeguards are implemented to protect personal information and health information which are commensurate with the sensitivity of the information.

2.2 Desktops must use a unique username and password to login. When using a desktop managed by MedIT, each individual must have a unique MED ID and password. MED accounts will be set up and managed as per the MED Accounts Usage Policy. On desktops and devices which are not managed by MedIT, it is the user's responsibility to ensure unique IDs are used and managed locally on the user's device.

2.3 Desktops must have antivirus/antimalware software installed with automated definition updates with real-time scanning. MedIT managed desktops have antivirus/antimalware software pre-installed and configured with automated definition updates with real-time scanning. On unmanaged desktops, it is the user's responsibility

to ensure installation of antivirus/antimalware software with automated definition updates and real-time scanning.

2.4 Desktops must have local firewall protection and only allow necessary network access. MedIT managed desktops have centrally managed local firewalls with limited network access. On unmanaged desktops, it is the user's responsibility to install and configure a local firewall.

2.5 Desktop operating systems and applications must be patched regularly. MedIT managed desktops are patched on a monthly basis. On unmanaged desktops, it is the user's responsibility to ensure patches are regularly installed.

2.6 Ensure mobile devices, such as smartphones, tablets and laptop computers, containing Health Information have encryption enabled and meet the standard of protection set out in University policies and procedures, including the UAPPOL Encryption Procedure and the FoMD Encryption Policy. The UAPPOL Encryption Procedure requires that all mobile computing devices used to store University personal information or confidential information be encrypted and protected in accordance with the standards developed by the Office of the Vice-Provost and Associate Vice-President (Information Technology). Mobile devices containing Health Information should be encrypted and protected to the same standards.

Additional requirements include mobile computing devices to run a current, fully patched and modern operating system, and be configured to ask for a password after a period of inactivity. The FoMD Encryption Procedure mandates that all personal computers storing sensitive information must be encrypted. The University's Mobile Computing Security website has information on other recommended controls for safeguarding against the risks of mobile computing.

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

2.8 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. MedIT managed desktops have screensaver locks configured for 15 minutes. On unmanaged desktops, it's the user's responsibility to ensure screensaver locks are appropriately configured.

2.9 Health Information will not be sent via e-mail without the use of appropriate security measures such as encryption. For information on how to encrypt attachments to e-mails, see the Information & Privacy Office's encryption website. This requirement applies to the transmission of records containing Health Information from a scanning or printing device to an email address or network folder.

2.10 Health Information to be encrypted must comply with the University and FoMD's encryption policies. USB devices shall be used in accordance with the FoMD USB Device Usage Policy.

2.11 When using an AHS managed computer or when using AHS health information systems, Health Information must be protected as per AHS corporate policies, procedures and directives.

2.12 When using Health Information in a shared electronic medical or dental record, the user shall comply with the policies, procedures and standards around the use of that system. Use of the provincial Electronic Health Record (i.e. Netcare) will be done in compliance with the HIA and Alberta Health or Alberta Health Services policies.

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 containing Health Information will be housed in a locked room or in locked cabinets inaccessible to the public.

3.2 Clinical areas and staff offices 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 is housed, including Health Information contained on computers or other electronic devices. 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. An 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. See the FoMD Physical Security Policy and its associated procedures for more information.

3.4 Buildings or areas that contain Health Information or computer equipment must be protected by adequate security measures.

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

3.6 Health Information that is physically 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 containing Health Information 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. Such cover sheets will not contain any identifiable Health Information. Fax transmissions may be sent directly from an electronic medical or dental record system. In such cases, numbers will be verified before being entered into the fax directory. Reasonable steps will be taken to confirm that any 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 depending on who the Custodian of the Health Information is, and any applicable Information Manager Agreements.

3.9 All FoMD computer equipment will be physically secured to standards set by FoMD MedIT. Portable computers, tablets, smart phones and other such electronic devices shall be stored in a locked cabinet or room 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 physical records containing identifiable Health Information will be destroyed by shredding or placed in approved shredding bins.

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

4 Mandatory Breach Reporting

4.1 Affiliates must notify the Custodian of any Breach of Health Information.

4.2 When a Custodian becomes aware of a Breach, it must determine whether a Breach gives rise to a "risk of harm" to the affected individuals. Some factors to consider in determining whether there is a risk of harm include whether there is a reasonable basis to believe that the Breached Health Information:

- May have been accessed or disclosed without authorization,
- Has been or will be misused,
- Could be used for the purpose of identity theft or to commit fraud, or
- Could cause embarrassment or physical, mental, financial or reputational harm to the affected individual.

4.3 If the Custodian determines there is a risk of harm under section 4.2 above, it must provide notification of the Breach to:

- The affected individual(s),
- The OIPC, and

- The Minister of Health,

subject to section 4.4, below.

4.4 A Custodian may not have to provide notification of a Breach under section 4.3 above if it can demonstrate:

- The Breached information was encrypted or otherwise secured in a manner which prevented unauthorized access or rendered the information unintelligible, or was destroyed before it could be accessed, or
- That whomever accessed or received the Health Information was a Custodian or Affiliate who is subject to appropriate privacy policies, accessed the Health Information in accordance with normal duties, and did not use or disclose the Health Information (except to identify and confirm the Breach and take reasonable steps to address it).

5 Transitory Records

5.1 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 as soon as they have fulfilled their purpose. In the event there is a reasonably anticipated or an actual legal action, or a request for information under the HIA, FOIP or other applicable privacy legislation, the destruction of all relevant records including transitory records must cease until the legal action or request for information is resolved.

5.2 Types of transitory records that are relevant to this procedure include:

- 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, and dictated audio records that have been transcribed.
- Draft documents that do not contain substantive new information or new approvals or decisions, including source materials used in preparation of documents, draft reports, or earlier versions of completed documents.

5.3 Records containing Health Information that are scanned into an electronic medical or dental record system, or other electronic records or clinical information system, will be retained according to the applicable standards of practice, code of conduct or other regulatory obligations published by the respective regulatory body of which the Custodian is a member (e.g. College of Physician and Surgeons of Alberta Patient Record Retention Standard). Retention after scanning and before destruction will ensure that the scan is of sufficient quality and the information has been effectively backed up by the system. Adequate quality assurance processes must be in place before scanned documents can be destroyed, such as having periodic documented quality checks.

5.4 Where practical, transitory records will be kept separate from records retained for business or legal purposes while in use.

5.5 Transitory records containing Health Information will be shredded in accordance with section 3.11 above.

DEFINITIONS

Affiliates	Includes all employees, volunteers, students, residents, fellows and persons contracted to provide services for Custodians. Physicians might also function as affiliates in their capacity of providing health services on behalf of Alberta Health Services and/or Covenant Health.
Breach	Refers to any loss of identifiable Health Information or other confidential information, or any unauthorized access to or disclosure of

	identifiable Health Information or other confidential information.
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 and its regulations.
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: diagnostic, treatment and care information; registration information (e.g. demographics, residency, health services eligibility, or billing).
Non-identifying health information	Information in which the identity of an individual cannot be readily ascertained.

Record	Means a record of health information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any information that is written, photographed, recorded or stored in any manner.
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
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 staff and students).
Use	Means applying health information for a purpose and includes reproducing the information, but does not include disclosing the information.

Related Links

College of Physicians and Surgeons of Alberta Patient Record Retention Standard of Practice

Information Privacy Office - HIA webpage

Faculty of Medicine & Dentistry - Informatics webpage

Health Information Act

Health Information Act Designation Regulation

Health Information Act Alberta Electronic Health Record Regulation

Health Information Regulation

Health Information Act Guidelines and Practices (Alberta Health)

Use and Disclosure of Health Information for Research (OIPC)