Protecting Personal and Health Information at the University of Alberta

Here are some highlights and quick tips on how to protect the privacy and security of personal and health information that you use when you work or volunteer for the University of Alberta. For more information, please take a look at the Information Privacy Office (IPO) website, attend an IPO training session, or contact the IPO.

In your affiliation with the University of Alberta you may come into contact with sensitive confidential information including "personal and health information" belonging to students, employees, patients, health care providers or the public. This is not an exhaustive list, but rather a few important things to know:

Privacy Laws

1. There are two privacy laws that govern the information stored at the University of Alberta: *Freedom of Information and Protection of Privacy Act* (FOIPP) and the *Health Information Act* (HIA). A resource is available that describes the differences between these two Acts and when to apply them. For more information on these Acts and how they apply to the University of Alberta please visit the IPO website at http://www.ipo.ualberta.ca/ and http://www.ipo.ualberta.ca/Health-Information-Act/Comparing-the-Acts.aspx

Privacy Training

2. Privacy and security training should be taken at the time of hire. You may need different types of privacy training depending on your role at the U of A and some information may overlap.

   a. U of A requirements are defined in the Access and Protection of Privacy Procedure https://policiesonline.ualberta.ca/PoliciesProcedures/Procedures/Information-Access-and-Protection-of-Privacy-Procedure.pdf.

   b. The University of Alberta privacy and security training can be found on the IPO website or by going here: https://privacyandsecurity.ualberta.ca/

   c. The University privacy and security acknowledgement must be completed annually, and can also be found at https://privacyandsecurity.ualberta.ca/.

   d. If you are handling health information, be sure to take Health Information Act training every one to three years, depending on the guidance you receive from your Faculty. Contact your Faculty to see which HIA training course is appropriate.
   **For those who work closely with AHS, the AHS HIA training can be found here: http://www4.albertahealthservices.ca/HIA_Awareness/index.html*

   e. Check with your Faculty and Department if you are unsure what training you are required to take.

Privacy Principles

3. Respect the privacy of others and safeguard personal information as if it was your own.

4. Only collect, use, and access the least amount of information needed to perform your assigned duties. Ask yourself, is this something I "need to know" or is it something "nice to know"? For example, if you only need someone's age, collect that rather than their birthdate.

5. When you collect health information, be sure to provide a notice of collection in compliance with the privacy legislation. See the following links for samples of appropriate notification statements:

- FOIPP Notification Statement http://www.ipo.ualberta.ca/FOIPP-Act/Guidelines/FOIPP-Notification-Statement.aspx
- HIA Notification Statement http://www.ipo.ualberta.ca/Health-Information-Act/HIA-Guidelines/HIA-Notification-Statement.aspx

6. Only disclose personal and/or health information if it is consistent with why you collected it, if you have the person's written consent, or as otherwise authorized by law. Consent forms must meet the requirements under law. See the following links for more information on consent requirements:
   - FOIPP consent http://www.ipo.ualberta.ca/FOIPP-Act/Guidelines/Informed-Consent.aspx
   - HIA consent http://www.ipo.ualberta.ca/Health-Information-Act/HIA-Guidelines/Consent.aspx

7. Disclosure of personal or health information must meet the requirements under privacy legislation.
   - Only disclose the **least amount of information** necessary.
   - Health information can be disclosed in certain situations without consent. For example, a custodian can disclose health information to other health care providers without consent for the purposes of continuing treatment and care.

8. Health information systems are audited. Ensure you are following the rules of the system.
   - Netcare privacy and security: http://www.albertanetcare.ca/PrivacySecurity.htm
   - eClinician Information Exchange Protocol http://www.albertahealthservices.ca/Assets/info/hp/iso/if-hp-iso-isf-emr-iep.pdf

   a. Both systems only allow users to access health information for the purpose of completing their job duties. Just because you have access to information doesn't give you the right to access or use this information outside of your job requirements.

   b. Only access or attempt to access health information that is required for the sole purpose of completing your assigned duties. This will include your own health information, or the information pertaining to: a family member, friend, colleague, or any person(s) known and/or unknown to you who is not within the scope of your job duties and responsibilities. Accessing or using information outside of your job duties is considered a breach of privacy legislation.

   c. **Don't snoop!** Information systems including those systems that manage health information are audited for inappropriate use. Failing to abide by the obligations and procedures set out in the Confidentiality Acknowledgement document constitutes misconduct which may be addressed under the applicable collective agreement and/or University policies. If you snoop or misuse personal or health information, you can also be personally fined under the *Freedom of Information and Protection of Privacy Act or* the *Health Information Act*.

   d. If a family member or close personal friend attends the clinic where you work, talk to your supervisor about the appropriate way of handling your family member's or friend's health information. Booking a family member or close friend may trigger an audit and perceived as potential queue jumping.

Note: Just because you have access to information through your job, it doesn't necessarily give you the right to look at the information for the sake of curiosity. Only access personal information if/when it is needed to do your job.

Example: *Updating your information in Bear Tracks would be appropriate as it is your personal information and not related to how you do your job; however, looking yourself up in an electronic medical record system is not appropriate. If you are asked by family and friends to look up their personal information from work resources to circumvent regular processes or give them extra information, this would not be considered an* *appropriate use; they should receive their personal information in the same way that any other member of the public receives personal information.*

9. Take reasonable steps to make sure that personal or health information is accurate and complete before you rely on it to make a decision that affects someone. If the personal or health information you have about someone is wrong, that person has the right to have the information corrected.

Safeguarding Information

10. Personal and individually identifying health information is considered confidential information and must be protected appropriately.
    - Personal and health information should be stored in a manner that allows only those with a **need to know** to access that information.

    - Password protection is not encryption. Use both password protection and encryption on mobile devices where health information is accessed or stored. http://www.vpit.ualberta.ca/security/

    - Be sure the way you store and transmit health information is an approved method. Store and transport the **minimum amount** of personal information necessary. https://www.vpit.ualberta.ca/encryption/docs/UofA_Email_Best_Practices.pdf

    - **Health information must be encrypted in transit**. Remember that email is not a secure way to transmit health information unless it is encrypted. http://www.ipo.ualberta.ca/FOIPP-Act/Guidelines/Privacy-Breach-Prevention/Encryption.aspx.

    - When faxing - double check number/e-mail address to be sure it is accurate. Use secure fax procedures http://www.ipo.ualberta.ca/Health-Information-Act/HIA-Resources.aspx

    - **Lock your computer** when you step away from your desk and log out of applications when you leave for the day.

    - **Information classification** is used to determine what level of security is required to appropriately protect a document https://www.vpit.ualberta.ca/encryption/docs/UofA_Email_Best_Practices.pdf

    - To consider information de-identified or non-identifiable, you must strip enough identifiers to adequately reduce the potential of someone re-engineering the data. When in doubt, treat as confidential.

    - Under the HIA, a **privacy impact assessment** must be submitted to the Office of the Information and Privacy Commissioner before using a new administrative practice or a new technology or information system to manage health information.

Important Policies and Procedures

11. It is important to safeguard and physically secure all health information, whether the information is stored on paper or electronic. You must make yourself aware of all University policies regarding protection of privacy, information security, and the acceptable use of information technology.

    o Information and Privacy Office http://www.ipo.ualberta.ca/FOIPP-Act/Policies-and-Procedures.aspx
    o Relevant Faculty, Department or Clinic’s governance material (i.e. Internal policies, procedures, standards, processes).

12. Retain and dispose of personal and health information records in a secure manner. See records policies and/or contact the University of Alberta's Records Officer. Shred paper records when disposing of them. Do not put in recycle or regular garbage. Make sure you securely wipe electronic devices.

13. You are required by law and by policy to report suspected or realized privacy/security breaches as soon as possible. Notify your direct supervisor and the IPO immediately as per the Responding to and Reporting of Information Security Breaches Procedure http://www.ipo.ualberta.ca/FOIPP-Act/~/media/ipo/Policies%20and%20Procedures/Responding-to-and-Reporting-of-Information-Security-Breaches-Procedure.pdf

*****Any unauthorized or inappropriate access, use, or disclosure of health information or personal information could result in investigation by any of the following entities: University of Alberta, Office of the Information & Privacy Commissioner, and any health authority whose IT system or facilities you are using (e.g. AHS). Each of these entities may implement a range of sanctions or penalties, independent of one another, which may include but are not limited to removal or suspension of all access privileges to health information or personal information, financial penalty and termination of employment.*

14. Contracts with third parties who will have access to personal or health information must be reviewed by the IPO http://www.ipo.ualberta.ca/~/media/ipo/Policies%20and%20Procedures/Contract-Review-Procedure.pdf. For example, before you use a new application to manage personal and/or health information, a privacy review must be completed.

Faculty of Medicine & Dentistry Quick Links:

For the employees in the Faculty of Medicine & Dentistry, here are some resources you may be interested in:

- Contact MedIT help desk if you have any questions regarding the transmission or storage of health information. http://medit.med.ualberta.ca/Pages/default.aspx
- Contact the Faculty of Medicine & Dentistry Health Information Privacy Advisor with privacy questions http://www.ipo.ualberta.ca/Information-and-Privacy-Office/Contact-Information.aspx
- Review Faculty of Medicine & Dentistry policies and procedures including a section on Information & Privacy and IT Security http://www.med.ualberta.ca/about/policies
- Check out the Faculty of Medicine & Dentistry Informatics website https://www.med.ualberta.ca/about/informatics
- Faculty of Medicine & Dentistry HIA Awareness Training and Quiz https://moodle.med.ualberta.ca/course/view.php?id=578