Privacy Continuing Competency Activity

Registrant Reminder

Section 3.4 of the Standards of Practice and Statement 4 of the Code of Ethics for the Profession

3.4 Protects the patient's right to autonomy, respect, confidentiality and access to information, in accordance with applicable federal and provincial legislation.

Statement 3 Each RRT shall keep in confidence all privileged patient information. Each RRT shall collect and disseminate patient information in accordance with federal and provincial legislation.

Introduction

This year's mandatory continuing competency activity on privacy legislation for respiratory therapists is a result of multiple complaints, received by the college's complaints director regarding registrant's involvement in unauthorized access to patient health records for purposes other than providing care to their patients.

With the introduction of the electronic health record and Alberta Netcare access to confidential patient health information has never been more convenient. Inherent with this convenient access is the potential for risks to patients if their information is used for purposes other than for the purposes the information was collected for which is healthcare.

Many registrants work for both the public and independent sectors and should be aware of the privacy legislation governing both sectors. It is not the intention of this learning activity to make you an expert on privacy legislation but rather provide a broad overview and understanding on the importance of the various *Acts* and *Regulations* that govern privacy for patients as well as the public.

Some of the complaints received are pursuant with section 57 of the *Health Professions Act* from employers who have taken disciplinary action against employees for contravening their policies and procedures for snooping and others by patients who were informed of their health information being accessed without authorization as required by the *Health Information Act (HIA)*.

On June 11th, 2025, the *Freedom of Information and Protection of Privacy Act* (FOIP) was repealed and replaced by two new Acts or laws: *Access to Information Act (ATIA)* for records access and the *Protection of Privacy Act (POPA)* for personal information

protection, modernizing rules for public bodies and enhancing transparency and privacy rights.

Key changes apply to public bodies aiming for greater openness and better data stewardship. They include:

1. Split legislation- two specific laws for access and privacy.
2. Modernization- aligns Alberta with global best practices and support digital government.
3. Stronger Privacy- POPA introduces stricter privacy protections, including a ban on selling personal information and enhanced data management.
4. New Timelines- the ATIA sets new response timelines for access requests (thirty business days).

Principles of the ATIA

1. Any person has a right of access to the records in the custody or under the control of a public body subject to specific and limited exceptions.
2. Allows individuals a right to access personal information about themselves, subject to specific and limited exceptions.
3. Provides for independent reviews of decisions made by public bodies and resolution of complaints under the ATIA.

ATIA Regulations

There are 2 supporting regulations that establish administrative and procedural requirements of the ATIA:

- *Access to Information Regulation*, authorized by the Lieutenant Governor in Council, integrates access to information related provisions from the former FOIP Regulation and incorporates new and revised provisions to provide clarity and outline additional information to support the updated legislative requirements under the ATIA.
- *The Designation of Public Bodies Regulation*, under the authority of the Minister of Service Alberta and Red Tape Reduction, is a list of entities that may not definitively meet the requirements established in the ATIA definition of a 'public body' and need to be explicitly designated (such as, by name) as a public body in this Regulation.

The ATIA and regulations work together to provide detailed, practical guidance to help public bodies implement the new rules.

POPA

POPA introduces a privacy by design approach to programs and services delivered by public bodies, has the strictest penalties in Canada for the misuse of Albertan's personal information, and supports more effective delivery of programs and services across public bodies by allowing for common and integrated programs.

The purpose of POPA is to:

1. provide guidance to the collection, use, and disclosure of personal information by public bodies.
2. allow individuals the right to request corrections to their personal information held by a public body.
3. enable public bodies to data match and allow the creation, use, and disclose of non-personal data and data derived from personal information.
4. require public bodies to protect personal information including when data matching, and creating, using, and disclosure of data derived from personal information and non-personal data.
5. allow for independent review of decisions made and resolution of complaints made against public bodies.

POPA prohibits the selling of personal information in any circumstances or for any purpose, including for marketing or advertising.

Regulations

The Protection of Privacy Regulation provides definitions for terms captured in the *Protection of Privacy Act,* and the Protection of Privacy (Ministerial) Regulation provides specific requirements for concepts captured in the Act, like the privacy management program and privacy impact assessments.

The Act and regulations work together to provide detailed, practical guidance to help public bodies implement the new rules.

Health Information Act

This Act governs and regulates access to and the collection, use and disclosure of health information. It provides Albertans with the right to access their own health information and

to request corrections. The Act also regulates the information accessible through Alberta's Electronic Health Record (Alberta Netcare). It protects the privacy and confidentiality of health information and enables health information to be accessed and shared to provide health services and manage the health system.

Patient's Rights

The *Health Information Act* (HIA) strikes a balance between the protection of privacy and enabling the appropriate amount of information sharing to provide health services and manage the health system.

Under the HIA, you have a right to:

- access a copy of your health information held by a custodian, subject to specific and limited exemptions.
- request a correction or amendment of your health information held by a custodian.
- protect your health information and understand the collection, use and disclosure of that information.
- know why your health information is being collected, used and disclosed.
- make an expressed wish regarding the disclosure of your health information – a custodian is required to consider your concerns before disclosing your health information.
- request an independent review of decisions made by a custodian regarding access to your information or a correction or amendment to your health information, within 60 days of being notified of the decision.

Personal Information Protection Act (PIPA)

PIPA applies to provincially regulated private sector organizations, businesses and, in some instances, to non-profit organizations for the protection of personal information and to provide a right of access to an individual's personal information.

Organizations that are subject to PIPA must develop and follow policies that are reasonable to meet its obligations under the act.

When PIPA refers to any thing or any matter as 'reasonable,' it is that which a reasonable person would consider appropriate in the circumstances.

Examples of common privacy breaches

Privacy breaches occur in a number of ways. Human error and malicious actions by threat actors can cause privacy breaches. A cybersecurity incident such as a ransomware or phishing attack may lead to privacy breaches if personal information is lost, accessed or disclosed as a result of the incident. Some common privacy breaches that have been reported to the Privacy Commissioner include: • Loss or theft of unencrypted mobile devices (e.g. laptops, USB sticks or hard drives) containing personal information. • Misdirected communications (via email, fax or mail) containing personal information. • Snooping of (unauthorized access to) patient or customer records by employees (authorized users). • Ransomware attacks resulting in exfiltration of personal information from a computer system and/or the encryption of the information within the compromised systems thereby preventing authorized users from accessing the information. • Insecurely disposing of paper records containing personal information by putting the records in a dumpster. • Disposing of computer systems or storage media without first securely removing personal information stored in them. • Stolen paper records containing personal information following a break-in into an office, employee's vehicle or a storage facility. • Break-in into a record storage facility where paper records containing personal information may not be stolen but accessed by the unauthorized individuals. • Inadvertent exposure of personal information over the internet due to system misconfiguration.

Consider Patient Consequences of Privacy Breaches

In the experience of the complaints director most consequences of privacy breaches on patients are immediate and impactful. Patients, disappointed managers and employers have indicated the feeling of being violated, their trust and confidence in the profession being broken and may never recover. One thoughtless or careless act (human error) leading to a privacy breach can have significant impact on a patient's well being and health. Please be careful not casual with patient's health information.

Safeguards for Registrants

The patient professional relationship is incumbent on respect for the privacy of the patient information collected, secure storage, appropriate access and disclosure for the delivery of safe, effective, and quality healthcare. It is highly recommended by the complaints director that as part of your ongoing continuing competency each year you take some time to review and refresh your understanding of your employer's privacy policies, procedures and any changes in response to recent amendments to privacy legislation in the province.

Virtual Respiratory Care

With the emergence of virtual meeting technology there are a host of potential privacy matters that need to be addressed before any patient care can be safely provided. The most notable requirement is a privacy impact assessment reported to the Office of the Information and Privacy Commissioner (OIPC).

Conducting a privacy impact assessment (PIA) helps to identify and address potential privacy and security risks that may occur when processing personal or health information as part of an electronic information system, administrative practice, data-matching or in other circumstances where risks to privacy may result from the processing.

Generally, a PIA maps the flow of information in a proposed system or practice and identifies the legal authority permitting it. A PIA also identifies privacy and security risks and associated mitigating controls.

Custodians under the *Health Information Act* (HIA) and **public bodies** under the *Protection of Privacy Act* (POPA) **are required in certain circumstances to complete a PIA** and submit it to the Commissioner for review and comment.

There is no such requirement in the *Personal Information Protection Act* (PIPA) for private sector organizations, although it is recommended that organizations complete a PIA as a best practice to mitigate any risks of non-compliance concerning the processing of personal information in electronic systems or administrative practices.

Resources

1) Health Information Act Guide for Custodians https://oipc.ab.ca/wp-content/uploads/2022/02/HIA-Guide-2010.pdf
2) Procedures for Reviews and Privacy Complaints https://oipc.ab.ca/resource/procedures-reviews-privacy-complaints-settlement-atia-popa/
3) Privacy Breach Response and Notification (Public and Private Sector) https://oipc.ab.ca/resource/privacy-breach-response/
4) Privacy Impact Assessments https://oipc.ab.ca/privacy-impact-assessments/
5) HIA https://kings-printer.alberta.ca/1266.cfm?page=h05.cfm&leg_type=Acts&isbncln=978077985806
6) ATIA https://kings-printer.alberta.ca/1266.cfm?page=a01p4.cfm&leg_type=Acts&isbncln=9780779857661

7) POPA https://kings-printer.alberta.ca/1266.cfm?page=p28p5.cfm&leg_type=Acts&isbncln=9780779856954
8) PIPA https://kings-printer.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779856701