

QUICK TIPS: TRAINING STAFF ABOUT PRIVACY

Privacy training for the entire team is one of the most critical safeguards to protect a clinic against breaches. The Privacy Officer is the contact for [privacy requirements](#) and training for the clinic. These tips will help privacy officers make sure that all new staff and physicians are well-informed about the privacy obligations under the Health Information Act and how these are implemented in your clinic.

PRIVACY TRAINING

Understanding privacy and security is a necessity for clinic teams. Privacy training teaches everyone how to apply best practices to their daily workflow and specific aspects of their roles. A key aspect of training includes knowing how to safeguard information when collecting, using, disclosing, and disposing of health information.

ONLINE PRIVACY TRAINING

[AMA's privacy training](#) is available for **all clinic staff** and volunteers, free of charge via Learn@AMA.

THE ESSENTIALS

Handling health information is a big part of physicians' and clinic staff's daily work. Whether you access the privacy training from the AMA or develop your own, these are the key items that your clinic team need to know about privacy in Alberta:

- Different types of information such as health, personal and business information
- Health Information Act basics
- Key privacy contacts in Alberta such as the [Office of the Information and Privacy Commissioner of Alberta](#) (OIPC), [Alberta Health](#) and the [College of Physicians and Surgeons of Alberta](#) (CPSA)
- Responsibilities of custodians and affiliates
- Ways to protect privacy during the collection, use and disclosure of health information
- Understanding the five privacy principles
 1. Need-to-know basis
 2. Highest level of anonymity
 3. Least amount of information
 4. Consent and notification
 5. Legal authority to release individually identifying information
- How to prevent, identify and report a breach
- Most common safeguards (Physical, Administrative and Technical)
- Clinic-specific policies and procedures
- Any changes to the legislation

YOUR CLINIC'S SAFEGUARDS

Safeguards are measures taken to protect against privacy and security incidents. Safeguards are commonly put into three categories - physical, administrative, and technical. A good way to remember these are you give yourself a PAT on the back! The PAT safeguards are considered best practices and should be implemented and reinforced with all staff (new and existing).



PHYSICAL

- Physically securing portable electronic devices and locking them when not in use. Store devices in a locked or secure area.
- Installing keypads and alarms for after-hours access. Staff have individually assigned passcodes and/or keys.
- Positioning computer terminals and fax machines so they cannot be seen or accessed by unauthorized users.
- Staff members accompany patients and visitors to examining rooms, offices and non-public areas of the clinic.
- Playing music or TV in the waiting room to limit overhearing of health information.



ADMINISTRATIVE

- Adhering to policies and procedures.
- A password policy such as using long and strong passwords. Use a combination of numbers and symbols or passphrases.
- Confidentiality agreements are signed and understood by all staff.
- Providing new users with system user training and advising them of confidentiality requirements before they are given access to the clinic EMR or Alberta Netcare. You can limit their access to only pertinent information about a specific patient's care that they are involved in.



TECHNICAL

- Provide education or training on phishing emails.
- Use unique login credentials for every employee.
- Do not store personal or health information on mobile computing devices unless needed.
- Limiting the use of the internet to clinic-related tasks.

TEN PRIVACY TIPS TO IMPLEMENT TODAY!

Start incorporating these tips today to increase your team's awareness about privacy and start embedding privacy into everyone's daily workflow.

1 Sign up your entire team for privacy training. Training should be provided to new employees as well as refreshed annually. Make sure that everyone gets training before handling health information.

2 Ensure that the team knows where the clinic privacy policies and procedures are kept. Give everyone time to review them.

3 Incorporate privacy tasks into your clinic's daily task checklist. For example, remove all confidential information from your desk, lock all computers at the end of the day, and check all the doors to make sure they are locked.

4 Post regular privacy updates on your staff bulletin board.

5 Set aside five minutes at each team meeting to review new privacy matters.

6 Create privacy routines that everyone follows such as a clean desk and locking up devices.

7 Teach all team members to treat patient privacy as if it was their own information.

8 Remind everyone of physical, administrative and technical (PAT) safeguards and make it everyone's job to make sure they are in place.

9 Take the opportunity to educate staff on recent news of privacy incidents.

10 Take advantage of learning tools and resources provided by credible sources such as AMA, AH, OIPC and CPSA.