cpsa
COLLEGE OF PHYSICIANS & SURGEONS OF ALBERTA

ADVICE TO THE PROFESSION

Lost or Stolen Patient Records

The College of Physicians & Surgeons of Alberta (CPSA) provides advice to the profession to support physicians in implementing the CPSA Standards of Practice. This advice does not define a standard of practice, nor should it be interpreted as legal advice.

Advice to the Profession documents are dynamic and may be edited or updated for clarity at any time. Please refer back to these articles regularly to ensure you are aware of the most recent advice. Major changes will be communicated to our members; however, minor edits may only be noted within the documents.

Physicians have an ethical and legal responsibility to safeguard their patients' information, including reporting any unauthorized access to or disclosure of individually identifying health information by themselves or their affiliates[1].

Privacy breaches can occur in a number of ways. Some of the more common incidents include:

- Loss or theft of mobile devices (e.g. laptops, USB sticks)
- Misdirected communications (via email, fax or mail) • Employee "snooping" of patient or customer records (also known as unauthorized access to or misuse of customer or patient information by an employee)
- Hacking of computers, servers and websites
- Malicious software ("malware") attacks, including ransomware
- Phishing or social engineering attacks
- Failure to wipe hard drives of computers and other devices prior to being resold

[1] Per section 60.1(1)-(3) of the *Health Information Act* (pages 48-49).

- Stolen paper records from an employee's vehicle, home or office
- Improper disposal of records or devices

When safeguards fail and patient files are lost or stolen or a privacy breach occurs, however, physicians have a responsibility to take the following steps without delay:

1. Assess the loss

a. What type of information?

b. How many patients affected?

c. Sensitivity/potential for misuse of the information

d. What type of harm could result (breach of privacy, physical harm, identity theft, etc.)

2. Notify the Office of the Information and Privacy Commissioner (OIPC)

A reporting form is available on the OIPC website. The Reporting a Breach to the Commissioner practice note has helpful information on how to proceed with this step.

See also: Key Steps in Responding to Privacy Breaches

3. Notify the police if appropriate, especially if there is physical property (such as a computer laptop or prescription pads) stolen.

4. Notify the CPSA

We may be contacted by patients and/or the media and would like to be able to respond appropriately and knowledgeably. Additionally, we may be able to offer more specific advice on the situation.

If TPP pads were lost or stolen, contact the TPP Department at CPSA so the prescription numbers can be invalidated and pharmacies notified.

5. Notify the patients affected by the loss
How and when to do this may depend on the number and the degree of loss (e.g. if the patient's entire chart, including their contact information, is stolen, it may make locating them much more difficult).

6. Ordinarily the CMPA (or other liability protection providers) need not be notified, unless the loss is significant or unusually sensitive, but members may wish to seek advice or legal assistance.

7. Take positive steps to prevent a similar loss in the future:

a. additional physical or technical security

b. refined procedures or processes

c. staff awareness/training measures

d. consider or review insurance coverage for such losses

RELATED STANDARDS OF PRACTICE

- *Code of Ethics & Professionalism*
- *Patient Record Retention*
- *Responsibility for a Medical Practice*

COMPANION RESOURCES

- Advice to the Profession documents:
  - Electronic Communications & Security of Mobile Devices
  - Physicians as Custodians of Patient Records
  - CMPA's Duties and Responsibilities: The new reality of reporting a privacy breach