MED THREE INSURANCE GROUP

106 Front St. East, suite 303
Toronto, ON M5A 1E1
Main: 416.477.2353
Fax: 416.477.2399

PART II - HEALTHCARE PRIVACY BREACHES: SAFEGUARDS AND MITIGATION STRATEGIES

What is a Privacy Breach?

In the healthcare context, a privacy breach occurs when there is unauthorized collection, use, disclosure, retention and/or disposal of personal health information. A privacy breach may occur through employees, third parties, or as a result of criminal activity. Some examples of instances that could result in disclosure of personal health information to unauthorized persons include:

- Theft or loss of a memory stick, laptop, iPad or smartphone etc. containing personal health information;
- Failing to shred documents containing personal health information that are no longer required; or,
- Mistakenly sending documents containing personal health information to the wrong fax number, email address or mailing address.

Safeguards

An organization must make reasonable efforts to ensure that records containing personal health information are protected against theft, loss and unauthorized use or disclosure as well as unauthorized copying, modification or disposal. Some safeguards to consider include:

- Increasing physical security by installing security alarms and security lighting;
- Limiting employee access to health records and restricting editing rights;
- Using password protection and auto-lock on all computers and electronic devices and regularly updating anti-virus software;
- Encrypting electronic records (the process of encoding data in such a way that third parties cannot view it);
- Storing records in locked cabinets or in a secured area and returning records to their cabinet as soon as possible after use;
- Implementing office policies regarding what information may be faxed and what measures should be taken to confirm fax numbers in advance;
- Implementing office policies regulating or restricting the use of personal smartphones, laptops, tablets, and personal email addresses for the receipt or transfer of personal health information;
- When transferring records containing personal health information, using couriers with a tracking system, requiring a signature for delivery and providing the recipient with a detailed list of the records being sent so that any missing records can be readily identified;
- Ensuring that paper records that are no longer required are shredded; and,
- Ensuring that electronic records that are no longer required are securely ‘wiped’ from computers and other electronic devices (iPad, laptop, smartphone, memory stick etc.).

Getting Prepared

1. Appoint a privacy officer and create a privacy breach response team;
2. Educate staff about privacy legislation and obligations;
3. Establish a contingency plan for responding to privacy breaches;
   - Become familiar with your notification obligations under the applicable legislation;
   - Delegate responsibilities to team members; and,
4. Rehearse responding to a privacy breach.

What to Do When a Privacy Breach Occurs

If you think a privacy breach has occurred, immediate action must be taken.

1. *Take immediate action to contain the breach*
   - Make efforts to recover the records that were improperly disclosed;
   - Secure all other records to prevent further unauthorized disclosure (i.e. change passwords, shut down the system etc.).
2. *Investigate the breach*
   - Keep a record of the circumstances in which the breach occurred;
   - Identify what personal health information may have been compromised;
   - Identify the individuals affected by the breach.
3. *Consider whether to notify your provincial privacy commissioner's office*
   - Investigate whether your province has mandatory privacy-breach notification requirements;
   - Contact your broker and consider legal advice to determine the scope of the obligation to notify[1];
   - The privacy commissioner can provide advice and assistance to an organization in responding to a breach.[2]
4. *Consider whether to notify the affected individuals*
   - Investigate whether your province has mandatory privacy-breach notification requirements;
   - Contact your broker and consider legal advice to determine the scope of the obligation to notify[3];
   - Consider the sensitivity of the information, the number of individuals affected and the risk and seriousness of potential harm;
   - Any notification should be done directly (i.e. letter, telephone, in person) and should include the following:
     a. A description of the privacy breach;
     b. A description of the personal health information that was compromised;
     c. A description of the remedial actions taken by the organization to address the breach;
     d. Advice about what individuals can do to protect themselves from the risk of harm;
     e. List a contact person at the organization who can provide further assistance and information.
5. *Remediation & Prevention*
   - Conduct an internal investigation into the breach and identify deficiencies in existing privacy policies and procedures;
   - Update privacy policies and procedures and implement appropriate safeguards;
   - Ensure that all staff have appropriate training with respect to privacy obligations;
   - Ensure that front-line staff are prepared to answer questions about the breach or have been instructed to refer inquiries to the organization's privacy officer or other designated person.

For more information on the privacy rules in your province, contact your provincial privacy commissioner's office or seek the advice of a lawyer.

[1] The scope of the obligation varies provincially, with a variety of factors to be considered and weighed. While mandatory requirements cannot be ignored, caution should be exercised before taking any steps that could prejudice your insurer and potentially compromise your insurance coverage.

[2] These are not protected communications, and could result in an investigation.

[3] The scope of the obligation varies provincially, with a variety of factors to be considered and weighed. While mandatory requirements cannot be ignored, caution should be exercised before taking any steps that could prejudice your insurer and potentially compromise your insurance coverage.

MedThree Insurance Group PrivaSure™ Privacy and Data Protection Program

The resources expended by organizations in implementing best practices for the prevention of privacy breaches pales in comparison with the exorbitant costs entailed in managing and mitigating a privacy breach. One rising consideration in risk management is the purchase of privacy liability insurance. MedThree Insurance Group offers such coverage through its PrivaSure™ Privacy and Data Protection Program.

PrivaSure™ coverage includes: damages that arise out of unauthorized use of, or tampering with all forms of private or public data; crisis management and public relations; regulatory action defense expenses; and computer system extortion expenses and losses. For further information on MedThree's PrivaSure™ product, please contact Andree Pinheiro at 416 408 5656.

Valerie Wise
Wise Health Law
416 915 4234
vwise@wisehealthlaw.ca