MED THREE INSURANCE GROUP

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

HEALTHCARE PRIVACY BREACHES – UNDERSTANDING THE RISK
Part 1: Privacy Breaches

As recent news stories of privacy breaches have shown, data security and privacy protection are critical public relations and business issue for Canadian healthcare organizations. *Privacy Breaches*, Part 1 and Part 2, provide:

1. brief overview of the relevant privacy legislation;
2. outline key steps an organization should consider when a privacy breach is discovered, and
3. suggest practices an organization should implement to manage privacy risks.

Understanding the Risk

" Norfolk General Hospital notifies 1,300 of privacy breach" *Brantford Expositor*, August 14, 2013.

"Patients Sue Montfort for $40M" *Ottawa Sun*, May 10, 2013

"Peterborough Regional Health Centre privacy victims file $5.6M lawsuit over employees snooping their medical records" *Peterborough Examiner*, March 26, 2013.

Privacy protection has become a hot topic in recent years, due mainly to the increasing complexity and interconnectedness of information technologies and to the millions of individuals in North America who have found themselves victims of privacy breaches as a result. The above cases are some of the most recent Canadian instances of healthcare data breaches this year. While some cases demonstrate the different types of hard costs (such as fines, penalties and defense costs) organizations risk suffering in the wake of privacy breaches, what these numbers do not reflect is the internal costs of rectifying such breaches, nor the loss of goodwill and bad publicity suffered by these organizations.

Legislative Backdrop

Canada has two federal privacy laws, the *Privacy Act* (http://laws-lois.justice.gc.ca/PDF/P-21.pdf) and the *Personal Information Protection and Electronic Documents Act* (http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf). The *Privacy Act* protects the privacy of individuals with respect to personal information about themselves held by a public sector institution (as defined by the legislation), and provides individuals with a right of access to that information. Personal information is information about an identifiable individual, recorded in any form, such as: an individual's home address, age or marital status; and health; and personal identification numbers, such as social insurance number or a bank account number.

The Privacy Act requires government institutions to define, and notify individuals of the lawful, authorized purposes for collecting their personal information. The Act imposes obligations on these institutions to respect privacy rights by limiting the collection, use and disclosure of personal information under their control. Personal information may only be disclosed with the consent of the individual to whom that information relates subject to defined and limited exceptions. The legislation gives individuals the right to access and to request correction of their personal information held by a government institution; however, access to personal information that relates to the individual's physical or mental health may be denied where it is felt this would not be in the best interests of the individual.

Individuals are also protected by the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA applies to private sector organizations, and requires their privacy framework to comply with the ten (10) fair information management principles of the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN-CSA-Q830-96). Key among the requirements of the Model Code is that organizations protect personal information with security safeguards appropriate to the sensitivity of the information; the more sensitive the data (e.g., medical and financial information), the higher the level of protection required.

All provinces and territories have enacted, or in the process of enacting privacy legislation. They all have the similar foundational requirements for: consent; reasonable safeguards; recommendations on privacy impact assessments; and access to and correction of personal information. The co-existence of federal and provincial legislation may mean that some personal information practices will be subject to both PIPEDA and applicable provincial legislation. It is, therefore, critical that a healthcare organization knows which privacy legislation applies to it and to its practice.

Safeguarding Personal Health Information

Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia have also each passed **health information protection** legislation to deal specifically with the collection, use and disclosure of personal health information by custodians or trustees (organizations or individuals who have possession of personal health information), and to individuals and organizations that receive personal health information from health information custodians. Subject to limited and specific exceptions, each statute contains provisions: entitling individuals to access their personal health information; limits access to and use of health information within a custodian's organization; and prohibits disclosure for purposes other than those to which an individual has consented.

As the custodian/trustee of personal health information, a healthcare organization is expected to have policies and procedures in place that, as a minimum, comply with the legislation in their jurisdiction, and that protect the confidentiality of that information and the privacy of individuals. The security measures outlined in *A Hospital Privacy Toolkit, Guide to the Ontario Personal Health Information Act, 2004* provide custodians or trustees with a starting point in the identification of safeguards for protecting personal health information:

(http://www.oha.com/KnowledgeCentre/Library/Toolkits/PublishingImages/Hospital%20Privacy%20Toolkit.pdf).

Understanding Privacy Breaches

A privacy breach is an incident involving unauthorized disclosure of personal information. A breach may be intentional or inadvertent, or as a result of criminal activity. A privacy breach may be the result of inadvertent errors or malicious actions. A breach may also be one-time occurrence (such as loss of a data stick), or due to systemic breakdowns (such as faulty procedure). Some of the most common privacy breaches occur when personal information is: stolen (e.g., theft of a computer containing patient files); lost (e.g., laptop containing personal information is left on a bus);mistakenly disclosed (e.g., personal information is mistakenly faxed to the wrong person).

Part 2 of this series addresses breach response management, and mitigation strategies.

© 2014 MedThree Insurance Group. All rights reserved.