Tips to help you protect your patients' personal information

Canadians are concerned about their personal information. In fact, according to a 2007 survey conducted on behalf of the Office of the Privacy Commissioner of Canada, 60% of Canadians think that health information is one of the most important types of personal information that need protection through privacy laws.

Further, Canadians fear that their personal information isn't as safe as it used to be. According to that same survey, seven of 10 Canadians feel they have less protection of their personal information than they did 10 years ago.

The following outlines some best practices and tips used by ICBC for managing documents that contain personal information. If you have not yet done so, I would encourage you to incorporate some of these tips into your practice. By having the proper controls in place, you reduce your risk of a privacy breach.

Collecting personal information

One of the biggest challenges facing businesses is tracking personal information—how it's collected, used, and stored, and who has access to it. Without this knowledge, it's hard for a business to determine if their documents are properly protected and in compliance with privacy law, policies, and best practices.

It may be helpful to consider conducting a risk assessment to evaluate your current practices, determine your legal requirements, and identify steps you can take to mitigate risk.

Start by determining what information is collected and stored (a data inventory). Initial questions should include:

- What kinds of data are you collecting (patient? employee?)
- Why are the data collected?
- How and where is the information stored?
- Who has access to personal information?
- How is authority to access the data controlled or supervised?
- Who can make changes to the data?

Copying documents

Every time you make a copy or send a copy of a document, the risk grows of someone stealing or using it for an unauthorized purpose. A simple best practice is to only make or share documents when required.

Sending personal data

Day-to-day business practices often require that patient information be sent via fax, e-mail, regular mail, and courier. Using the example of a patient with an ICBC claim, there may be an exchange between the adjuster, family physician, other health care providers, the patient, and lawyers. Every time this sensitive information is transmitted, there's a risk that it may be inadvertently disclosed or exposed to theft.

Best practices suggest sending the information in a manner that is commensurate with the sensitivity of the information, and having safeguards in place to ensure that the information makes it to its destination.

Personal information should not be sent by fax unless it is necessary to transmit the information quickly. It is important that sufficient precautions are taken to ensure that it is received only by its intended recipient.

Out of the office

If documents containing personal information are taken out of the office, for example a file is stored electronically on a laptop, take all necessary precautions to protect the information from theft. Consider the following:

Canadians fear that their personal information isn't as safe as it used to be.

- Laptop theft is often a crime of convenience. Laptop computers are prime targets for thieves, especially in offices that are open to the public. Never leave a laptop unattended or unlocked in an unsecured environment.
- Use encryption software on laptops that contain personal information.
- Back it up. This way, any personal information lost can be easily identified and the affected parties can be promptly notified.
- When a breach occurs, inform your patients immediately.
- Employees entrusted with laptops containing personal information should be regularly reminded of your privacy protection policies and procedures.

Storage and destruction

The storage and disposal of documents is another potential access point for identity thieves. Ask yourself:

- How secure are your storage areas?
- How do you manage who has access to these storage areas?

While oftentimes data breaches involve stolen laptops or a break-in, they could also result from "dumpster diving." In these situations, documents are discarded without being properly destroyed and therefore are an easy find for identity thieves. Never discard documents where they could be accessed by others.

For more information

British Columbia's Office of the Information and Privacy Commissioner

Continued →