

Breaches of Privacy in the Health Care System

Thomas Macmillan
December 2017

The Ontario Information and Privacy Commissioner will soon have a lot more data on actual or potential privacy breaches, thanks to a new regulation which affects health care providers.

In response to some relatively high-profile breaches of individuals' health and personal information, Regulation 224/17 to the *Personal Health Information Protection Act, 2004* imposes additional requirements on "health information custodians," a category of entities that includes pharmacies, health care practitioners, home care providers, hospitals, laboratories, and retirement homes.

The Regulation came into force on October 1, 2017.

The new Regulations do not expand on the existing precautionary steps that health information custodians must take to protect the personal health information of individuals. Rather, the changes impose new obligations to report actual or potential privacy breaches.

Report to Commissioner

A health information custodian must now report to the Commissioner when the custodian has reasonable grounds to believe that any of the following has taken place with respect to personal health information in its custody or control:

- that it was used or disclosed without authority; or
- that it was stolen.

In addition, the custodian must report to the Commissioner if it has reason to believe that any loss or unauthorized use or disclosure is part of a pattern of losses. A custodian must also report to the Commissioner if it considers the breach to be significant, due to it relating to:

- sensitive information;
- a large volume of information;
- information from a large number of individuals; or
- the involvement of more than one health information custodian or agent in the loss.

Custodians had previously been required to notify individuals, within 30 days, in the event of a loss or unauthorized use or disclosure of personal health information. Now, however, the Commissioner must also be put on notice.

Report to College

Furthermore, custodians must now also report to a professional College in the event that an employee who is a member of the College is either terminated, suspended, resigns, or is the subject of disciplinary action related to the actual or suspected loss or unauthorized use or disclosure of personal health information.

Annual Report

Starting on March 1, 2018, custodians must keep track of each instance of a breach of personal health information. An annual report must be filed by custodians, setting out the number of breaches. The first report is to be filed on March 1, 2019.

Impact

Most health information custodians already have in place the necessary mechanisms for tracking actual or potential privacy breaches, and have been reporting such breaches to individuals.

What is new is an increased concern by custodians of attracting unwanted attention from the Commissioner. It can and should be assumed that focus will be paid to the annual reports, and those custodians with less than stellar figures can expect to hear from the Commissioner.

It can also be assumed that the Office of the Commissioner will take these changes as a mandate to be more proactive. The message to the health care industry with the passage of these new Regulations is that Province is unhappy with the level of compliance with existing privacy laws, and that it plans on more closely monitoring the landscape.