ONTARIO HOSPITAL ASSOCIATION

200 Front Street West, Ste. 2800
Toronto, ON M5V 3L1
Tel: 416 205 1300
Fax: 416 205 1360
www.oha.com

LEGISLATIVE UPDATE

March 2017

Backgrounder

Proposed Regulation on Mandatory Reporting of Privacy Breaches

Context

On March 10, 2017, the government released a proposed regulation on mandatory reporting of privacy breaches for public consultation. The proposed provisions would amend O. Reg 329/04 under the *Personal Health Information Protection Act, 2004* (*PHIPA*), to require both statistical reporting and point-in-time reporting to the Information and Privacy Commissioner of Ontario (IPC).

The proposed regulation applies to all health information custodians (HICs), as defined under section 3 PHIPA to include any individual or organization "who has custody and control of personal health information" (PHI) for purposes related to the Act.

Click here to view a copy of the Ministry of Health and Long-Term Care's consultation document for this regulatory proposal.

Key Highlights of the Proposed Regulation

- The regulation would introduce a requirement for HICs to report annually to the IPC on the number of times the HIC had to notify affected individuals of thefts, losses and unauthorized uses or disclosures of PHI in a calendar year.
- The IPC would be permitted to require additional information regarding these notifications, including the content of the notice, and the information relied upon in deciding to notify affected individuals.
- Point-in-time reporting of privacy breaches to the IPC would also be introduced through the proposed regulations. There are a number of prescribed circumstances which would trigger a reporting obligation.

Regulatory Amendments Relating to Mandatory Reporting of Privacy Breaches

The regulation proposes to introduce two types of mandatory reporting relating to privacy breaches:

A. Annual Statistical Reporting

PHIPA currently requires HICs to notify affected individuals at the first reasonable opportunity if their PHI is stolen or lost, or if it is used or disclosed without authority. The proposed regulation would require that all HICs track the number of such notifications to affected individuals in a calendar year, and provide this information on an annual basis to the IPC.

The first annual report would be required by **March 1, 2019**, for the 2018 calendar year.

After the report is submitted, the proposed regulation would require HICs to provide specified information upon request by the IPC. The information requested by the IPC may include:

- Information contained in the notice given to affected individuals when PHI is stolen, lost or used or disclosed without authority; and
- Information that the HIC relied on in deciding to notify affected individuals that their PHI was stolen, lost or used or disclosed without authority.

As a reminder, in accordance with the *Freedom of Information and Protection of Privacy Act* (*FIPPA*), hospitals are also required to report annually to the IPC in a number of other areas, including the number of requests for access to records under *FIPPA* and *PHIPA*.

B. Point-in-Time Reporting

In addition to annual reporting, the proposed regulation would require that all HICs notify the IPC of privacy breaches that meet the prescribed requirements set out in the proposed regulation.

A HIC would be required to report a privacy breach to the IPC in **any** of the following circumstances:

1. The HIC has reasonable grounds to believe that the PHI that was stolen, lost or used or disclosed without authority has been or will be subsequently used or disclosed without authority.

2. The theft, loss or unauthorized use or disclosure is part of a pattern of similar thefts, losses or unauthorized uses or disclosures of PHI under the custody or control of the HIC.

3. The HIC has given notice to a regulated health professions college ("RHP college"), or to the Ontario College of Social Workers and Social Service Workers (OCSWSSW), concerning a member who is an employee or an agent of the HIC, under **any** of the following circumstances:

    a. The employee or agent has been terminated, suspended, or subject to disciplinary action as a result of the employee or agent's unauthorized collection, disclosure, retention or disposal of PHI;
    b. The employee or agent resigns, and the HIC has reasonable grounds to believe that the resignation is related to an investigation or other action by the HIC with respect to alleged unauthorized collection, disclosure, retention or disposal of PHI;
    c. The member's affiliation or privileges with the HIC are revoked, suspended or restricted, as a result of unauthorized collection, disclosure, retention or disposal of PHI by the member; or
    d. The member voluntarily relinquishes or restricts his or her privileges or affiliation with the HIC, and the HIC has reasonable grounds to believe that this relinquishment or restriction is related to an investigation or other action by the HIC with respect to alleged unauthorized collection, disclosure, retention or disposal of PHI.

4. With respect to other agents of the HIC who are not members of a RHP college or the OCSWSSW, where any of the circumstances under 3(a) or 3(b) are met.

5. The HIC has reasonable grounds to believe that the PHI was intentionally used or disclosed without authority.

6. The circumstances do not meet the requirements in any of the preceding paragraphs, and the HIC determines that the theft, loss or unauthorized use or disclosure is significant having regard to all relevant circumstances including:

    a. The nature of the PHI that was stolen, lost or used or disclosed without authority;
    b. The number of records of PHI that were stolen, lost or used or disclosed without authority;
    c. The number of individuals whose PHI was contained in the record or records that were stolen, lost or used or disclosed without authority; and
    d. The number of HICs or agents responsible for the theft, loss or unauthorized use or disclosure.

No particular form or further details around the content of the reporting notice to the IPC are currently provided in the proposed regulations.

The requirements around point-in-time reporting would take effect on **July 1, 2017**.

Additional Information and Next Steps

In accordance with the requirements under PHIPA, a mandatory 60-day consultation period on these proposed regulations will conclude on **May 8, 2017**.

The OHA is assessing the potential impact of the proposed regulations, and will be preparing a submission to government on behalf of members.

For more information, please contact Melissa Prokopy, Director, Legislative, Legal and Professional Issues at 416 205 1565 or mprokopy@oha.com or Alice Betancourt, Legal and Policy Advisor at 416 205 1359 or abetancourt@oha.com