[4] Level of Harm Required to Notify

Chapter 5 Breach

§ 5.02 Regulatory Landscape

[4] Level of Harm Required to Notify

Although not always expressed in the same terms, most Access to Information and Personal Information Protection Legislation and most PHI legislation set certain thresholds below which a breach does not have to be notified. This threshold in Saskatchewan FIPPA is "real risk of significant harm,"[1] or "a risk of serious injury" in Québec.[2] Invariably, the assessment as to whether the breach will cause a real risk of significant harm requires an analysis as well as a judgment call that can be very subjective. To assist Entities, Saskatchewan's Office of the Information and Privacy Commissioner provides the following items to consider when determining if the breach has a real risk of significant harm:

- Who obtained or could have obtained access to the information?
- Is there a security measure in place to prevent unauthorized access, such as encryption?
- Is the information highly sensitive?
- How long was the information exposed?
- Is there evidence of malicious intent or purpose associated with the breach, such as theft, hacking, or malware?
- Could the information be used for criminal purposes, such as for identity theft or fraud?
- Was the information recovered?
- How many individuals are affected by the breach?
- Are there vulnerable individuals involved, such as youth or seniors?[3]

Another approach is that adopted by Ontario *Personal Health Information Protection Act*[4] ("PHIPA") that requires the individual to be notified if their information suffers a breach but that makes notification to the Commissioner mandatory only if certain circumstances contained in the Regulation are met.[5] These conditions are essentially the same as those that should lead an Entity to conclude that the breach poses a real risk of significant harm. The advantage of this approach is that there is less room for discretion.

Footnote(s)

1 *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F-22.01, s. 29.1.

2 *An Act respecting Access to documents held by public bodies and the Protection of personal information*, CQLR, c. A-2.1, s. 63(6).

3 Office of the Saskatchewan Information and Privacy Commissioner, “Real Risk of Significant Harm” (January 2, 2018), online: https://oipc.sk.ca/real-risk-of-significant-harm/.

4 *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A.

5 *General*, O. Reg. 329/04, s. 6.3(1):

> 6.3(1) …
>
> 1. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing the information without authority.
> 2. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was stolen.
> 3. The health information custodian has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in the custodian's custody or control, the personal health information was or will be further used or disclosed without authority.
> 4. The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information in the custody or control of the health information custodian.
> 5. The health information custodian is required to give notice to a College of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.
> 6. The health information custodian would be required to give notice to a College, if an agent of the health information custodian were a member of the College, of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.
> 7. The health information custodian determines that the loss or unauthorized use or disclosure of personal health information is significant after considering all relevant circumstances, including the following:
>
> i. Whether the personal health information that was lost or used or disclosed without authority is sensitive.
>
> ii. Whether the loss or unauthorized use or disclosure involved a large volume of personal health information.
>
> iii. Whether the loss or unauthorized use or disclosure involved many individuals’ personal health information.
>
> iv. Whether more than one health information custodian or agent was responsible for the loss or unauthorized use or disclosure of the personal health information.