THE LAWYER'S DAILY

The Lawyer's Daily | 111 Gordon Baker Road, Suite 900 | Toronto, ON M2H 3R1 | www.thelawyersdaily.ca
Phone: (800) 668-6481 | Fax: (905) 479-3758 | John.Carson@lexisnexis.ca

Privacy Law

Complying with PIPEDA's new breach reporting rules

By **David Young**

David Young

(November 14, 2018, 9:26 AM EST) -- New rules under the federal privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), requiring reporting of breaches to the Office of the Privacy Commissioner and notification of affected persons, came into force on Nov. 1. The rules mandate reporting of any "breach of security safeguards" that meets the threshold of a "real risk of significant harm." PIPEDA's *Breach of Security Safeguards Regulations* set out the information that must be included in reports and notifications.

The threshold requirement for reporting (and notification) is that it is reasonable to conclude that there is a "real risk of significant harm to an individual." To assist, PIPEDA provides a non-exhaustive definition of "significant harm" and identifies factors relevant to making such determination. To further assist organizations in making this determination, at the end of October the OPC issued a guidance document — *What you need to know about mandatory reporting of breaches of security safeguards.* There, the OPC indicates that a *two-tier assessment* is required: firstly, the sensitivity of the information compromised and secondly, the probability of it being misused or wrongfully accessed.

As examples of sensitive information, the OPC refers to PIPEDA's Consent Principle — which cites medical and financial records. However, it also makes clear that sensitivity of information may be determined by its potential use or misuse; meaning, for example, that even a person's birthdate or home address might be considered sensitive where it could be combined with other information to enable identity fraud.

With regard to the second tier of the assessment — probability of misuse — the OPC provides a list of example questions, addressing the circumstances of the breach and issues such as the likelihood of anyone being harmed, who had access, the length of time the information was exposed and whether there was any malicious intent. Further questions address whether the information was password protected or encrypted or has been recovered.

The OPC's suggested approach to risk analysis is helpful but may not cast a sufficiently wide net in determining whether or not to report a breach or notify affected individuals.

There are many circumstances where a narrow focus on the nature of the information exposed or the causes of a breach may not register a "yes" to the OPC's questions, but which still could result in a significant risk. For example, an innocent error that leads to the exposure of identity information within a large group not otherwise considered potential misusers may pose a significant risk simply because of the possibility that there may be individuals in the group who might misuse the information.

The regulations also provide direction regarding the content of reports to the OPC, including the circumstances of the breach, the number of individuals affected and the steps that the organization is taking to reduce the risk of harm and to notify affected individuals. The OPC has provided an online form for making reports which while not mandatory, is useful in providing prepopulated fields and examples of the information expected to be included.

Notification of affected individuals must be made as soon as feasible after discovery of a breach and contain sufficient information to make them aware of the breach and take steps to reduce the risk. The regulations stipulate the minimum disclosure and the tracking that is required for reports to the OPC, with the added stipulation of providing guidance regarding the steps to be taken to reduce the risk of the harm.

Notification must be given directly to individuals — except if it would cause further harm to the individual, or be prohibitively expensive, or if the individual's contact information is not available — in which cases notification must be given indirectly, such as through public media channels.

If an organization determines that it must notify individuals, it also must notify any other organization or public body (such as law enforcement) that may be able to reduce or mitigate the risk.

In addition to the reporting obligation, the new rules require organizations to keep records of *all* breaches, whether or not they meet the threshold, for 24 months, in sufficient detail to enable the OPC to verify that the organization has complied with the mandatory reporting requirements. The OPC states that if the breach was not reported and individuals not notified, the record also should include a brief explanation of why it was determined that the risk threshold was not met.

The new PIPEDA rules establish quasi-criminal offences, punishable by fines, for organizations that knowingly breach the new reporting rules, including the record-keeping requirements. This potential exposure together with the increased public scrutiny, and potential lawsuits, that mandatory reporting will bring make it essential for all organizations to review their breach response protocols and institute adjustments and additional procedures where required.

In addition to establishing criteria and procedures for the new requirement to keep records, organizations will need to consider whether to retain their internal risk assessment information — such as gap analyses — beyond that required for making the reporting threshold determination. In light of the increased risk of reputational damage — and exposure to lawsuits — organizations will need to consider whether they should protect their internal investigations by means of legal privilege.

David Young is principal at David Young Law*, a privacy and regulatory counsel practice in Toronto.*

Photo credit / roberthyrons ISTOCKPHOTO.COM

Interested in writing for us? To learn more about how you can add your voice to The Lawyer's Daily*, contact Analysis Editor Richard Skinulis at* Richard.Skinulis@lexisnexis.ca *or call 437- 828-6772.*