i-SIGMA™

Home of NAID & PRISM International

CI– 009M
C.P. – PL 64
Protection des renseignements personnels

September 21, 2020

M. André Bachand, M.N.A.
Chair, Committee on Institutions
Via email: CI@assnat.qc.ca

Chèr M. Bachand:

On behalf of the International Secure Information Governance and Management Association (i-SIGMA), I would like to offer congratulations to the Province of Quebec for greatly advancing the debate around privacy with Bill 64. Canada used to be a global privacy leader, but that has waned considerably in recent years, so it is timely that Quebec has filled the void by introducing this important piece of legislation.

By way of background, i-SIGMA was created in May 2018 following the merger of the National Association for Information Destruction (NAID) and PRISM International (Professional Records and Information Services Management). NAID has always been the watchdog association for secure shredding operators worldwide and together with PRISM International the joint association now represents all four pillars of records and information management: physical records and information storage; data protection and media vaulting; digitizing and scanning; and confidential records and information destruction services. As such, i-SIGMA is the umbrella association for these professional privacy practices that stand united, heralding the proper information lifecycle management needed in today's regulatory climate.

Bill 64 presents the most sweeping changes to privacy legislation seen in Canada in decades and will provide Quebecers with more protections and greater control over their personal information, like is provided with Europe's General Data Protection Regulation. In effect, Bill 64 is going to set a new bar against which all other Canadian jurisdictions will be measured, and we have already cited it as a model in outreach to the Federal Government and other provinces.

The Bill includes several measures that i-SIGMA supports, including increased fines for privacy violations, breach notification requirements, and public disclosure of privacy policies and practices. We believe the latter in particular is a critical consumer confidence measure as it allows consumers to assess an organization's privacy policies and take their business to those they feel have the best practices.

Also, privacy legislation is only as effective as the degree to which organizations comply with it. Closely linked to that is the need to ensure employees understand and abide by the law. i-SIGMA has found that just having a policy does not necessarily translate into compliance if an organization's employees are not aware of it and/or do not adhere to it. Keys to the latter are awareness, proper and ongoing training and, where necessary, penalties for violations of the law. Many jurisdictions around the world are moving in this direction, recognizing that certain privacy violations warrant a punitive response.

i-SIGMA – Canada Office
190 O'Connor Street, 5th Floor, Ottawa, Ontario K2P 2R3
Phone: 613-241-6000, ext 223
www.isigmaonline.org

With fines, consider some examples from the U.S. related only to destruction, an area we follow closely through our NAID origins. A medical group in Massachusetts was fined US$140,000 for disposing of 67,000 patient records in a dump without any redacting or shredding.[1] In another case the U.S. Department of Health and Human Services reached an US$800,000 settlement with an Ohio company that left 5,000-8,000 patient records in the driveway of a physician.[2] Also in the U.S., the Federal Trade Commission fined a Las Vegas real estate broker US$35,000 for leaving 40 boxes of customer tax returns, bank statements, consumer reports and other financial records in a public dumpster.[3] Meanwhile, a Missouri medical company faced fines of up to US$1.5 million for leaving medical records in a public dumpster.[4]

Our one potential concern with Bill 64 is drawing a distinction between "destruction" and "anonymization" of information. We have always defined destruction as follows:

> *"Destruction" means the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information (or parts thereof) is not practical. "Destroy" means the act of destruction.*

This definition applies to both paper and electronic records, making it technology neutral. Variations of it have been incorporated into privacy legislation in a number of jurisdictions in Canada, the U.S. and around the world. Meanwhile, Bill 64 states that *"the person carrying on an enterprise must destroy or anonymize the information, subject to any preservation period provided for by an Act. For the purposes of this Act, information concerning a natural person is anonymized if it irreversibly no longer allows the person to be identified directly or indirectly."*

As your Committee studies this Bill, it would be worth clarifying whether blacking out the name on a medical or financial record constitutes "anonymization." In theory, the remaining information might make it impossible for another person to identify to whom the record is related, but I doubt anyone would be comfortable with this approach. In contrast, under our definition, "destruction" means the records and their personal information no longer exist, which would seem to be preferable.

Otherwise, Bill 64 is a welcome piece of legislation and we look forward to its passage. Thank you for your time and consideration, and please do not hesitate to contact me if you have questions.

Sincerely,

Tony Perrotta
Director, Canada, i-SIGMA
www.isigmaonline.org

[1] See https://nakedsecurity.sophos.com/2013/01/15/medical-patients-health-records-dump/
[2] See http://www.hhs.gov/about/news/2014/06/23/800000-hipaa-settlement-in-medical-records-dumping-case.html#
[3] See http://www.lexology.com/library/detail.aspx?g=5af8a709-0850-487d-bc74-4db192e80ff1
[4] See http://www.hipaajournal.com/hipaa-settlement-reached-dumpster-phi-exposure/