OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

News Release

February 1, 2023

Mandatory breach reporting and privacy management program requirements now in effect for public bodies

VICTORIA— Public bodies are now required to develop privacy management programs and report privacy breaches that could be expected to result in serious harm.

The new requirements, which were among amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA) enacted in November 2021, came into force today. They apply to the more than 2,900 public bodies covered by FIPPA.

Michael McEvoy, Information and Privacy Commissioner for British Columbia, welcomed the changes.

"The changes to FIPPA coming into effect today are ones for which my office has long advocated, and mark an important step forward for our province's public sector privacy law," said Commissioner McEvoy. "British Columbians can have greater confidence that when they entrust their personal information to public bodies, these entities have programs in place to protect that information, and that if a breach happens, no time will be wasted in informing them and our office so that we can all work to minimize harms."

Mandatory breach notification
Public bodies are now required to notify affected individuals and the OIPC of privacy breaches that could reasonably be expected to result in significant harm, without unreasonable delay. For more on this requirement, see *Privacy breaches: tools and resources for the public sector:* https://www.oipc.bc.ca/guidance-documents/3750

Privacy management programs
Public bodies are now required to develop privacy management programs that are "commensurate with the volume and sensitivity of the personal information in the public body's custody or under its control."

These programs must include:

1. Designation of someone responsible for privacy-related matters and the development, implementation and maintenance of privacy policies/procedures.
2. Process to complete and document privacy impact assessments and information-sharing agreements as appropriate under FIPPA.
3. Documented process for responding to privacy complaints and breaches.

4. Ongoing awareness/education on privacy activities for staff.
5. Privacy policies/documented privacy processes or practices available to employees and, where practicable, the public.
6. Methods to ensure service providers know privacy obligations.
7. Process to regularly monitor and update privacy management program as needed.

(This list is summarized from the Ministry of Citizens' Services' Privacy Management Program Direction. For full requirements, visit: https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/pmp_ministerial_direction_2023.pdf)

Media Contact
Michelle Mitchell | Senior Communications Manager
Office of the Information and Privacy Commissioner for BC
250 217-7872 | mmitchell@oipc.bc.ca
Twitter: @BCInfoPrivacy