Canadian and International Breach Reporting Obligations Comparison

By Timothy M. Banks, nNovation LLP

This document provides information about requirements in Canada to notify affected individuals and regulators about security breaches involving personal information collected in the course of commercial activities or in the health sector.

This document also provides users with a useful comparative reference to the European Union General Data Protection Directive, the Australia Privacy Act 1988, the U.S. Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule, the Federal Trade Commission (FTC) Breach Notification Rule, and the U.S. state laws of California and New York. It should be noted that all 50 U.S. states have laws, which differ in their details. California and New York are referenced for illustrative purposes only.

This is a summary only and does not contain all relevant details that may be necessary to determining an organization's legal compliance. The text of the applicable law should be referenced for details and legal advice sought from qualified legal advisors with respect to the application of these laws to particular circumstances. Note that data breach laws change frequently. **This comparison is prepared as of November 1, 2018**. Please check with Lexis Practice Advisor for updated and expanded comparisons as well as additional clarifications.

Laws & Official Regulatory Guidance

Canada

Personal Information Protection and Electronic Documents Act (Canada), S.C. 2000, c. 5

https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

Personal Information Protection Act (Alberta), S.A. 2003, c. P-6

https://www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx

Health information Act (Alberta), R.S.A. 2000, c. H-5

https://www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx

Personal Health Information Privacy and Access Act, S.N.B. 2009, c P-7.05

http://www.info-priv-nb.ca/forms-public-phi.asp

Personal Health Information Act, S.N.L. 2008, c. P-7.01
https://www.oipc.nl.ca/custodians/privacy-breach-report

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sch.A
https://www.ipc.on.ca/health/report-a-privacy-breach/

Australia

Privacy Act 1988, No. 119, 1988 (Australia)
https://www.oaic.gov.au/privacy-law/privacy-act/

Europe

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
UK Information Commission's Office: https://ico.org.uk/for-organisations/report-a-breach/

United States

Note all 50 U.S. States have laws.

California Civil Code, § 1798.80 et seq
https://oag.ca.gov/privacy/databreach/reporting

New York General Business Law § 899-aa
https://its.ny.gov/breach-notification

Health Insurance Portability and Accountability Act Breach Notification Rule, 45 CFR §§ 164.400-414
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

FTC Health Breach Notification Rule, 16 CFR Part 318
https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/health-breach-notification-rule

Personal Information Protection and Electronic Documents Act

Application
All organizations that collect, use or disclose personal information in the course of a commercial activity in Canada or with individuals in Canada except: (i) those organizations whose collection, use or disclosure takes place solely within British Columbia, Alberta or Quebec; and (ii) health information custodians in the provinces of Ontario, New Brunswick, Newfoundland and Nova Scotia with respect to the collection, use and disclosure of personal health information that occurs solely within their respective provinces. Also applies to federal works, undertakings and businesses that collect, use or disclose personal information in connection with applicants for employment or employees.

Covered Personal Information
Personal information means information about an identifiable individual (this includes information that could, if combined with other information, be used to identify the individual).

Definition of a Security Breach
A breach of security safeguards is the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards (physical, technical or organizational measures) that were in place or that should have been in place having regard to the sensitivity of the information.

Service Provider Obligations
None explicitly mentioned.

Individual Notification
An organization must notify affected individuals of any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. Notification must be made as soon as feasible after the organization determines the breach has occurred. Notification must contain prescribed information.

Regulator Notification
An organization must report to the Office of the Privacy Commissioner of Canada any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. Reports must be made as soon as feasible after the organization determines the breach has occurred. Reports must contain prescribed information.

Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Organizations must consider the sensitivity of the personal information and the probability that it has been, is being or will be misused when determining if there is a real risk of significant harm.

Third Party Notification
An organization must notify any other organization, a government institution or a part of a government institution of the breach if this would assist in reducing or mitigating the risk of harm.

Safe Harbours
None.

Private Right of Action
Individuals are not precluded from bringing an action.

Alberta Personal Information Protection Act

Application
General application to all companies, trade unions, and non-profits operating within Alberta or where there is a real and substantial connection between the activities with respect to personal information and Alberta. Also applies to individuals acting in a commercial capacity.

Covered Personal Information
Personal information means information about an identifiable individual (includes information that could, if combined with other information, be used to identify the individual).

Definition of a Security Breach
A loss of or unauthorized access to or disclosure of personal information.

Service Provider Obligations
None explicitly mentioned.

Individual Notification
If ordered by the Office of the Information and Privacy Commissioner of Alberta, the organization must notify the individual. Notifications must contain the prescribed information. Note: Ordinarily, organizations that believe the test has been met will proactively notify the affected individual before being ordered by the Commissioner to do so.

Regulator Notification
An organization must report to the Commissioner any incident involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure. Reports must contain the prescribed information and must be made without unreasonable delay.

Third Party Notification
None explicitly mentioned.

Safe Harbours
None.

Private Right of Action
Individuals are not precluded from bringing an action.

Australia Privacy Act 1988

Application
Businesses and not-for-profit organisations with an annual turnover of $3 million or more, credit reporting bodies, health service providers, and tax file number recipients, among others.

Covered Personal Information
Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Definition of a Security Breach
An "eligible data breach" is the loss of, unauthorized access to, unauthorized disclosure of personal information.

Service Provider Obligations
None expressly mentioned.

Individual Notification
An organization must notify affected individuals if the test for notification to the Commissioner is met. Notification must be made promptly and contain prescribed information.

Regulator Notification
An organization must notify the Office of the Australia Information Commissioner if a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates. If information has been lost, the organization must first determine whether the circumstances are such that the information is likely to be accessed or disclosed and then consider the risk of harm. Notification must be made as soon as practical in the prescribed form.

Third Party Notification
None explicitly mentioned.

Safe Harbours
If information is lost but steps are taken to prevent the unauthorized access or disclosure or to mitigate the harm such that the harms test is not met, the breach is not an "eligible breach" that must be reported to the Commissioner or notified to individuals.

Private Right of Action
Individuals are not precluded from bringing an action.

European Union General Data Protection Regulation (GDPR)

Application
Organizations that offer goods or services to data subjects in the European Union or monitor the behaviour of data subjects in the European Union.

Covered Personal Information
Personal data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of a Security Breach
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Service Provider Obligations
Data processors must notify the controller without undue delay after becoming aware of a personal data breach.

Individual Notification
Controllers must notify affected individuals if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. Notifications must be made without undue delay.

Regulator Notification
A controller must report to the data supervisory authority a personal data breach unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The report must be made without undue delay and, where feasible, not later than 72 hours after having become aware of it. Any reports later than 72 hours must be accompanied by reasons for the delay.

Third Party Notification
None expressly mentioned.

Safe Harbours
Notification is not required if the information was encrypted or protected by other methods that would render the personal data unintelligible.

Statutory Private Right of Action
Individuals are not precluded from bringing an action.

California Civil Code

Application
Organizations that do business in California and own or license computerized data that contains personal information.

Covered Personal Information
Personal information means: (1) an individual's name (first name and last name or first name initial and last name) in combination with social security number, driver's licence or state identification card number, account number, credit card number or debit card number and any required access code, medical information, health insurance information, or automated licence plate recognition system; or (2) an email address and password or security question.

Definition of a Security Breach
A security breach is a breach of security of the data of a resident of California involving personal information.

Service Provider Obligations
Service providers must notify the owner or licensee of the information that was the subject of the security breach immediately following the discovery that the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Individual Notification
Organizations must notify affected individuals if (1) the resident's unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or (2) the encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.

Regulator Notification
If a security breach affects more than 500 California residents, a copy (without individually identifying information) of the security breach notification must also be submitted to the Attorney General electronically.

Third Party Notification
None mentioned.

Safe Harbours
None.

Statutory Private Right of Action
Individuals may bring a civil action to recover damages.

New York General Business Law

Application
Organizations conducting business in New York state that own or licence computerized data.

Covered Personal Information
Two types of information are covered with different obligations – personal information and private information. Personal information means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. Private information means personal information (other than publicly available information) in combination with any of the following: social security number, driver's licence number or identification card number, account number, credit card or debit card number and any required access code.

Definition of a Security Breach
Breach of security of the system means unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.

Service Provider Obligations
Service providers must notify the owner or licensee of the information that was the subject of the security breach immediately following the discovery that the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Individual Notification
An individual must be notified of a breach of security if private information was, or is reasonably believed to have been, acquired by a person without valid authorization. Notifications must be made in the most expedient time and without unreasonable delay. Notifications must contain prescribed information.

Regulator Notification
If the test for individual notification is met, the organization must also notify the New York State Attorney General, the Department of State, and the State Police. Notifications to the Attorney General must contain the prescribed information.

Third Party Notification
If more than 5,000 New York State residents will be notified, the organization must also notify consumer reporting agencies.

Safe Harbours
Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

Statutory Private Right of Action
Individuals are not precluded from bringing an action.

Alberta Health Information Act

Application
Custodians of health information, which include (among others) hospitals, nursing home operators, ambulance operators, provincial health boards, regional health authorities, community health councils, regulated health providers (such as physicians, dentists, and others) and pharmacies.

Covered Personal Information
Individually identifying health information means diagnostic, treatment, care and registration information from which the identity of the individual could be readily ascertained.

Definition of a Security Breach
A security breach is the loss of, unauthorized access to or unauthorized disclosure of individually identifying health information.

Service Provider Obligations
Affiliates (e.g. employees and service providers) must notify the custodian of any security breach. The notification must be made as soon as practicable.

Individual Notification
If there is a risk of harm to an individual as a result of the security breach, the custodian must notify the individual. Notification must be given as soon as practicable and contain the prescribed information.

Regulator Notification
If there is a risk of harm to an individual as a result of the security breach, the custodian must notify the Information and Privacy Commissioner. Notification must be given as soon as practicable and contain the prescribed information in the prescribed form.

Third Party Notification
The custodian must notify the Minister of Health.

Safe Harbours
There are several possible safe harbours: effective encryption or other technological means to prevent access to the information or render it unintelligible; or a loss of information where the custodian can demonstrate the information was destroyed or rendered inaccessible or unintelligible; or recovery of information before it was accessed. There is also a safe harbour for inadvertent disclosure among custodians where the information was not used for an improper purpose.

Private Right of Action
Individuals are not precluded from bringing an action.

New Brunswick Personal Health Information Privacy and Access Act

Application
Custodians of personal health information, which include health care providers (such as physicians, dentists, massage therapists, and psychologists), hospitals, community health centres, pharmacies, laboratories, nursing homes, and regional health authorities.

Covered Personal Information
Personal health information means (among other things) identifying information about an individual that relates to the physical or mental health of the individual (including a family history), the providing of health care (including the identity of the provider), relates to testing of a body part or bodily substance, relates to the donation of a body part or bodily substance, payments or eligibility for healthcare or coverage for healthcare, the individual's health number or substitute decision maker.

Definition of a Security Breach
A security breach is the theft, loss, unauthorized access, unauthorized disclosure, or unlawful disposal of personal health information.

Service Provider Obligations
None explicitly mentioned.

Regulator Notification
The custodian must report the security breach to the Office of the Integrity Commissioner of the breach at the first reasonable opportunity.

Individual Notification
The custodian must provide notice to the individual at the first reasonable opportunity of a security breach. The custodian must provide prescribed information.

Third Party Notification
None mentioned.

Safe Harbours
No.

Private Right of Action
Individuals are not precluded from bringing an action.

Newfoundland & Labrador Personal Health Information Act

Application
Custodians of personal health information, which include health care providers (such as physicians, dentists, massage therapists, and psychologists), hospitals, community health centres, pharmacies, laboratories, nursing homes, and regional health authorities.

Covered Personal Information
Personal health information means (among other things) identifying information about an individual that relates to the physical or mental health of the individual (including a family history), the providing of health care (including the identity of the provider), relates to testing of a body part or bodily substance, relates to the donation of a body part or bodily substance, payments or eligibility for healthcare or coverage for healthcare, a drug, aid, device, product or other equipment provided under a prescription or other authorization issued by a health care professional or substitute decision maker.

Definition of a Security Breach
A security breach is the theft, loss, unauthorized access, unauthorized disclosure, or unlawful disposal of personal health information.

Service Provider Obligations
None expressly mentioned.

Regulator Notification
If the security breach is material, the custodian must inform the Information and Privacy Commissioner. In determining whether there is a material breach, the custodian should have regard to the sensitivity of the personal health information, the number of affected individuals, whether the custodian reasonably believes that the personal health information has been or will be misused, and whether the cause of the breach or pattern of breaches indicates a systemic problem.

Individual Notification
The custodian must provide notice to the individual at the first reasonable opportunity of a security breach. The custodian must provide prescribed information.

Third Party Notification
None mentioned.

Safe Harbours
No.

Private Right of Action
Individuals are not precluded from bringing an action.

Ontario Personal Health Information Protection Act, 2004

Application
Health information custodians, which include (among others) health care practitioners (such as physicians, nurses, dentists and pharmacists), hospitals, long-term care facilities, and ambulance services.

Covered Personal Information
Personal health information means (among other things) identifying information about an individual that relates to the physical or mental health of the individual (including a family history), the providing of health care (including the identity of the provider), relates to testing of a body part or bodily substance, relates to the donation of a body part or bodily substance, payments or eligibility for healthcare or coverage for healthcare, the individual's health number or substitute decision maker.

Definition of a Security Breach
A security breach is the theft, loss, unauthorized access or unauthorized disclosure of personal health information.

Service Provider Obligations
Health information network providers must notify a health information custodian at the first reasonably opportunity if an unauthorized person accessed the personal health information or the provider accessed, used, disclosed or disposed of personal health information other than in the course of providing the services for the health information custodian.

Regulator Notification
The custodian must notify the Information and Privacy Commissioner of a security breach involving personal information if (1) there are reasonable grounds to believe the personal health information was stolen or used or disclosed without authority by a person who knew or ought to have known they were using or disclosing the information without authority, (2) there are reasonable grounds to believe that the personal health information was or will be further used or disclosed without authority after the initial security breach, (3) the security breach is part of a pattern of similar security breaches, (4) an employee is terminated because of a security breach or resigns and there are reasons to believe the resignation is related to an investigation into a security breach, (5) the security breach is significant after considering all the relevant circumstances including the sensitivity of the information, the volume of information, the number of individuals, and whether more than one health information custodian or agent of the health information custodian was responsible for the security breach.

In addition, commencing March 1, 2019, health information custodians must make annual reports of the number of all security breaches in the prescribed form.

Individual Notification
The custodian must notify the individual of a security breach involving personal health information in the custodian's custody or control. The notification must be made at the first reasonable opportunity and contain prescribed information.

Third Party Notification
None mentioned.

Safe Harbours
No.

Private Right of Action
Individuals are not precluded from bringing an action.

U.S. Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule

Application
Covered entities, which include health plans, health care clearing houses and health care providers who transmit protected health information in electronic form, as well as business associates of covered entities. Business associates are persons (other than employees) that use or disclose of protected health information on behalf of, or provides services to, a covered entity.

Covered Personal Information
Protected health information is all individually identifiable health information held or transmitted by a covered entity or its business associate. Individually identifiable information is information that relates to the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

Definition of a Security Breach
Breach of security means the acquisition of unsecured information without the authorization of the individual. Unsecured means it was not protected using a technology or methodology specified by the Secretary of Health and Human Services.

Service Provider Obligations
Business associates must notify custodians of a security breach. Notice must be given without unreasonable delay and no later than 60 days after the breach is known or reasonably should have been known. There are prescribed method of notice and content requirements.

Regulator Notification
For security breaches affecting more than 500 individuals, the covered entity must provide notification to the Secretary of Health and Human Services without unreasonable delay and no later than 60 days after the breach is known or reasonably should have been known. For security breaches affecting less than 500 people, an annual report can be made. There are form and content requirements for the notice.

Individual Notification
Notice of a security breach must be given to affected individuals. Notice must be given without unreasonable delay and no later than 60 days after the breach is known or reasonably should have been known. There are prescribed methods of notice and content requirements.

Third Party Notification
If more than 500 residents of a state are involved, the covered entity must also notify prominent media outlets servicing the state without unreasonable delay and no later than 60 days after the breach is known or reasonably should have been known.

Safe Harbours
No.

Private Right of Action
Individuals are not precluded from bringing an action.

U.S. Federal Trade Commission Health Breach Notification Rule

Application
Applies to U.S. and foreign vendors of personal health records (health records that are managed, shared and controlled by or primarily for the individual), entities that offer products and services through the website of a vendor of personal health records, entities that access information in a personal health record or send information to a personal health record. This Rule does not apply to organizations that are covered entities under the Health Insurance Portability and Accountability Act Breach Notification Rule.

Covered Personal Information
Individually identifiable health information that identifies or could identify the individual and is created or received by a health care provider, health plan, employer or health care clearinghouse and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Definition of a Security Breach
Breach of security means the acquisition of unsecured information without the authorization of the individual. Unsecured means it was not protected using a technology or methodology specified by the Secretary of Health and Human Services.

Service Provider Obligations
Third party service providers must provide notice to the vendor of the health record. Notice must be given without unreasonable delay and no later than 60 days after the breach is known or reasonably should have been known.

Individual Notification
Notice of a security breach must be given to affected U.S. citizens or residents. Notice must be given without unreasonable delay and no later than 60 days after the breach is known or reasonably should have been known.

Regulator Notification
Notice of a security breach must be given to the Federal Trade Commission. Notice must be given without unreasonable delay and no later than 60 days after the breach is known or reasonably should have been known.

Third Party Notification
None mentioned.

Safe Harbours
No.

Private Right of Action
Individuals are not precluded from bringing an action.