Your Guide to HIPAA and Health Information Protection Acts

Author : Cat

Date : July 14, 2020

What is HIPAA?

HIPAA (often misspelled as HIPPA) is the *Health Insurance Portability and Accountability Act* of 1996. This US based law applies to how companies can collect, use, disclose, and store health related data. It also includes rules around how patients/individuals can get a copy of their own data and learn who else has accessed it.

Given the global nature of software, we often use ‘HIPAA Compliant’ as the standard of managing *digital* health data, but data that falls under the EU must meet GDPR Standards. Data that falls under Canadian jurisdiction must meet provincial regulations. In Canada, each province has their own personal health information act, detailed in the table below.

Province or Territory	Health Information Protection Act

British Columbia	E-Health Act (Personal Health Information Access and Protection of Privacy Act)
Alberta	Health Information Act
Saskatchewan	Health Information Protection Act
Manitoba	Personal Health Information Act
Ontario	Personal Health Information Protection Act
Quebec	An Act to amend the Act respecting health services and social services, the Health Insurance Act and the Régie de l'assurance maladie du Québec
Newfoundland & Labrador	Personal Health Information Act
Nova Scotia	Personal Health Information Act
New Brunswick	Personal Health Information Privacy and Access Act
PEI	Under Canada's PIPEDA
Yukon	Health Information Privacy and Management Act
Northwest Territories	Health Information Act
Nunavut	Under Canada's PIPEDA

Canadian Provincial Health Acts

Though the various regulations are nuanced in who can control and access data, and the time period to report breaches, the general guidance around high levels of privacy and security are the same. HIPAA has two specific sections that address these areas appropriately called the Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, and the Security Rule establishes a national set of security standards for protecting specific health information that is held or transferred in electronic form.

Definitions

Protected Health Information or Personal Health Information (PHI) – Information about an individual that discloses:

- Mental or physical condition (current and past, including family history)
- The provision of health care, including health care providers and health care coverage

- Government health number or identifying plan numbers

HIPAA uses ‘protected health information’; Canada uses ‘personal health information’.

Covered Entities – This is a term specific to HIPAA and refers to the person and/or entity responsible for the collection and handling of PHI. These entities include:

- A health plan
- A health care clearinghouse
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter

Health Information Custodians– This is a term is widely used by Canadian Acts and refers to the person or entity responsible for the collection and handling of PHI. Custodians are defined as:

- Operates an organization that provides health care to an individual
- Has custody or control of that individual’s personal health information.

Custodians include physicians, nurses, pharmacists, laboratories, ambulance services etc.

Right of Access – An individual has a right of access to obtain a copy of their protected health information and inspect it. There are exclusions, including medical opinions such as notes written by a psychotherapist.

Right to amend- An individual has the right to have a covered entity or custodian amend or correct protected health information.

Right to an accounting of disclosures of protected health information - An individual has a right to request and obtain a report of disclosures of their protected health information. Under HIPAA this request can be made of a covered entity covering the six years prior to the request date.

Security and Privacy

Personal Health Information is consider *Highly Sensitive* data and as such should be protected with the highest Privacy and Security Standards. *Security* highlights the protection of the data against unauthorized access and control. *Privacy* limits the availability of that data to those that need it. For example, security would protect a medical file from being accessed by the wrong doctor where as privacy would grant access to only the information that doctor needs.

HIPAA stipulates that **Covered Entities** must:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) *Risk management (Required).* Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Canadian legislations and GDPR are comparable. The risk assessment for GDPR is called the Data Protection Impact Assessment (DPIA) and in Canada we use the Privacy Impact Assessment (PIA). These are run on every new product and service.

To meet the standards above, there are three methods of securing information:

Administrative Safeguards

Administrative Safeguards are actions, policies and procedures that ensure that security measures are met. Under this umbrella are Risk Analysis, Information Access Management, Security Awareness Training and contingency plans including Disaster Recovery.

Physical Safeguards

Physical Safeguards includes limited and controlled access to facilities. Policies and controls around access to workstations, devices and media. Entities and custodians must also have a solid media deletion strategy that physically alters the devices.

Technical Safeguards

Technical Safeguards are software and firmware imposed restrictions on access including unique userIDs, automatic log off, and audit reports for tracking activity. Authentication is a key part of limiting access and should include multi-factor login where possible, especially if login is remote. Finally, encryption is recommended to protect information on transfer and storage.

Privacy Incident Response

A privacy incident is considered a breach when the data in question has been accessed in a way that is unauthorized. This can include unintentional acts like a medical file given to the wrong practitioner, a phone call with results made to the wrong patient, or a misplaced thumb drive. Breaches also cover serious attacks to a system such as ransomware or access by a criminal.

Under all regulations, individuals need to be notified if their data has been compromised.

For HIPAA, “a meaningful breach” is when more than 500 people are involved, and it must be reported within 60 days of discovery. For less than 500 people, it is consider “non-meaningful” and the covered entity has until 60 days after the calendar year,

In Canada, beaches are reported to individuals at the “first reasonable opportunity”. Notifications can be made by telephone, by writing, or even by making a note in their file (if low severity).

More Help and Information

More information on HIPAA can be found on the US Health and Human Services Website.

More information on the individual Canadian legislations can be found on the provincial pages (search by province).

For EU and GDPR guidance, visit our GDPR overview page.

If you want help from our consultants, have any questions or find something we've missed let us know!