FAQ's

1. What is the difference between HIPAA (US), GDPR (EU), PIPEDA (Canada), and Provincial Legislations (HIPA, etc)?

- HIPAA (US)

  HIPAA is a US federal law that governs the privacy and security of Personal Health Information (PHI) in the US.

- GDPR (EU)

  The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). Any entity entering into a business relationship with a EU entity is subject to GDPR.

- PIPEDA (Canada)[1]

  The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal privacy law for private-sector organizations in Canada. All businesses that operate in Canada and handle personal information that crosses provincial or national borders are subject to PIPEDA, regardless of the province or territory in which they are based (including provinces with substantially similar legislation).

- Provincial Legislations[2]
  - PIPA (BC), PIPA (AB), Privacy Act (QC)

    Private-sector privacy laws that have been declared substantially similar to PIPEDA. This means that these laws apply instead of PIPEDA in most cases.

  - PHIPA (Ont), PHIPAA (NB), PIHA (NL), PHIA (NS)

    Health-related privacy laws that have been declared substantially similar to PIPEDA with respect to health information.

  - HIPA (SK)

    Health-related privacy law, *not declared* substantially similar to PIPEDA. PIPEDA still applies to most cases in Saskatchewan.

---

[1] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

[2] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-3

FAQ's

2. What do Compliance, Privacy and Security mean?

Compliance, Privacy and Security are often used interchangeably but refer to different things:

- **Compliance** refers to an organization's adherence to laws, regulations, guidelines and specifications relevant to its business processes.
- **Privacy** in this context refers to how personal information is obtained, used, and protected.
- **Security** refers to protections of the platform, network, applications, operating system, physical infrastructure and data.
    - Common security programs include HITRUST CSF, NIST 800-53, ISO/IEC 27001/27002 and SOC3

3. What is encryption and what does it mean for compliance?

Encryption is the mathematical process by which a message or a piece of information is encoded, rendering it accessible and comprehensible only to the authorized people.

In the context of compliance, encryption of data at-rest (while not in use) and in-transit (while being transmitted) mitigates the effects of data security breaches, meaning that even if a piece of information was leaked, its content would be unintelligible to anyone unauthorized.

FAQ's

4. How do I know if a service is compliant (ie: can I use WhatsApp, FaceTime, etc. for TeleHealth in Canada?)

- There are no compliance certification programs by regulatory bodies for PIPEDA in Canada and there are no compliance certification programs by regulatory bodies for HIPAA in the US.[3]
- Some 3rd parties offer HIPAA (US) certifications, but these are not endorsed by any US governing body. Moreover, such certifications do not preclude a regulatory body from subsequently finding a security violation.[4]
- To know if a service is compliant it is important to consider:
    i. Where the service is located and what legislation applies to them and you
    ii. What is the Privacy Policy of the service (how do they obtain, use and protect personal information)
    iii. What are the security standards of the service
    iv. What are the Terms of Service for the service

5. What is a BAA?

A Business Associate Agreement (BAA) is a written arrangement between companies that specifies each party's responsibilities when it comes to handling Personal Health Information (PHI).

6. Do I need a BAA if I practice in Canada?

Canadian healthcare organizations can obtain some legal protection by signing a Business Associate Agreement (BAA) with a U.S.-based information service provider.[5] Typically BAAs are not signed between Canadian-based healthcare companies. It is important to note some service providers will not enter into a BAA (ex. Apple).

Additional guidance for security when working from home:
https://www.linkedin.com/pulse/cyber-security-remote-work-you-doing-right-daniel-gagnon/

Disclaimer: This information is provided for educational purposes only. The general information provided should not be interpreted, or used as a substitute, for professional, legal consultation. Practitioners are responsible for ensuring all legal compliance requirements for their practice.

---

[3] https://www.hhs.gov/hipaa/for-professionals/faq/2078/which-csps-offer-hipaa-compliant-cloud-services/index.html

[4] https://www.hhs.gov/hipaa/for-professionals/faq/2078/which-csps-offer-hipaa-compliant-cloud-services/index.html

[5] https://waelhassan.com/from-hipaa-to-phipa-baa/