

Privacy and Access Odds & Ends: 'HIPAA' Edition



What is HIPAA?

- The US Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, safeguards patient privacy and secures health information. This law sets strict standards for managing, transmitting, and storing protected health information in the United States. HIPAA applies to healthcare providers, insurers, and other organizations handling patient data, mandating safeguards to prevent unauthorized access or misuse of sensitive information.



Does HIPAA Impact How we Manage PHI at Health PEI?

- No. HIPAA is an Act specific to the United States, therefore, it is not relevant to personal health information (PHI) on PEI.
- While Canadian and American health privacy laws share the common goal of protecting patient data, they differ significantly in scope, application, and enforcement. There is no direct Canadian equivalent to the US HIPAA; instead, Canada uses a mix of federal and provincial law.

What Legislation Governs PHI in PEI?



- Since 2017, The **Health Information Act** (HIA) governs the collection, access, use, and disclosure of personal health information across the public and private health care sectors in PEI.
 - The principles upon which the Act is premised include:
 - protecting the privacy of individuals and the confidentiality of their PHI;
 - ensuring that PHI is shared appropriately; and
 - ensuring that records containing PHI are managed and protected appropriately.

If you're working on a project that is '**HIPAA compliant**' or '**General Data Protection Regulation (GDPR) compliant**', it may mean that a vendor or program has good privacy practices in place, however, we still need to ensure it complies with the HIA, often through a Privacy Impact Assessment (PIA).

To determine if a PIA is required for your project, please review the material on the Staff Resource Centre and reach out to the ATIP team at healthprivacy@ihis.org as needed.