Protecting ePHI
PIPEDA & HIPAA

As a health care practitioner you are responsible for the protection of patient privacy and the security of their personal data and health care records. Health care in Canada is covered under the Personal Information Protection and Electronic Documents Act (PIPEDA). The act has several provisions that protect the patient and obligations to which individuals and organizations in health care are bound. Similar legislation is found in the United States under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Verified Medical complies with both Acts to ensure that patient data is protected and to ensure continued confidence in the Verified Medical platform.

Core provisions of PIPEDA in Canada

- Consent must be garnered for collection of personal information
- Collection of personal information is limited to reasonable purposes
- Limits use and disclosure of personal information
- Limits access to personal information
- Stored personal information must be accurate and complete
- Designates the role of the Privacy Officer
- Policies and procedures for breaches of privacy
- Measures for resolution of complaints
- Special rules for employment relationships

Verified Medical helps healthcare professionals abide by the Act through:

- Ensuring patient personal information is used solely within the patient file
- Limiting use of patient information through secure sharing with pre-approved, trusted partners
- Limiting access to patient information by restricting access through roles and permissions

In addition, Verified Network Inc. has policies in place for the protection and management of breaches of privacy, a process to resolve complaints and policies regarding employee access to data held by clients. Our Privacy Officer is responsible for our compliance as a service provider, in addition to providing the security and privacy provisions through the Verified Medical platform.

HIPAA in the United States

In the US, privacy and security of patient information is governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), with stringent rules and procedures for managing patient information. HIPAA is a more comprehensive set of rules and guidelines for managing personal healthcare information (PHI) and includes:

- Limits to the use and disclosure of personal healthcare information (PHI):

  - a patient's name, address, birth date and Social Security number;

  - an individual's physical or mental health condition;

  - any care provided to an individual; or

  - information concerning the payment for the care provided to the individual that identifies the patient, or information for which there is a reasonable basis to believe could be used to identify the patient.

In addition, as an Information System holding PHI, Verified Medical meets the requirements for HIPAA as shown in the table overleaf.

How Verified Medical protects your data under HIPAA

The table below shows how Verified Medical complies with HIPAA in the US and some of the many steps we take to ensure continued compliance. We are constantly reviewing our security and privacy measures and update our policies and platform from time to time to reflect changes in security protocols, procedures and technological improvements.

Implement a means of access control	✓	Access to Verified Medical is by username and password authentication.
Introduce a mechanism to authenticate ePHI	✓ (in US)	Verified Medical does not directly interface with any US ePHI systems and does not need to authenticate ePHI. For US platforms we do have the ability to authenticate how ePHI information is entered and submitted.
Implement tools for encryption and decryption	✓	All data captured, stored and transmitted with Verified Medical is encrypted using banking grade encryption methods.
Introduce activity logs and audit controls	✓	All activity is logged within the Verified Medical platform, from file capture, up-load, manipulation and secure sharing.
Facilitate automatic log-off of PCs and devices	✓	Verified Medical will automatically log authenticated users out of the platform after a period of inactivity.
Facility access controls must be implemented	✓	Verified Medical holds patient information on our secure servers, located in a data warehouse in Ontario. The data warehouse has stringent access controls to ensure physical access to our server is restricted to authorized personnel.
Policies for the use/ positioning of workstations	✓	As with our mobile devices, Verified Medical can only be used on a limited number of devices at a given time. We have the ability to restrict the number of physical workstations and desktop devices that can access a user account.
Policies and procedures for mobile devices	✓	As with workstations and desktop devices,Verified Medical can only be used on a limited number of devices at a given time. We have the ability to restrict the number of mobile devices that can access a user account.
Inventory of hardware	✓	Verified Medical has a limited number of physical devices where ePHI data is stored. We maintain an inventory of these devices and audit them annually.
Conducting risk assessments	✓	The Verified Medical team conducts an annual risk assessment to determine what ePHI data is being stored and used and to examine where possible risk of data breach may occur.
Introducing a risk management policy	✓	Following our annual risk assessment audit, we review our procedures and patch our security and servers as necessary to ensure continued protection for our customers.
Training employees to be secure	✓	All Verified Medical staff, administrative and technical, go through a training procedure to understand what data we hold on behalf of our customers and to understand our security policies and procedures.
Developing a contingency plan	✓	In the event of an emergency, Verified Medical has a contingency plan to ensure the integrity of our data, and accessibility for our customers.
Testing of contingency plan	✓	We review our contingency plan periodically to ensure that it is feasible and would work if needed.
Restricting third-party access	✓	Using our robust security measures, roles and permissions, we restrict access to data to those who are authorized to use it. Third Party access is restricted to those who have been granted specific permission to access that data.
Reporting security incidents	✓	All security incidents are recorded and monitored.