HOSPICE DATA SECURITY GUIDE

SUMAC
By Silent Partner

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS

HIPAA COMPLIANCE
Health Insurance Portability and Accountability Act

DATA SECURITY & HOPICES

Because hospices deal with sensitive client information on a daily basis, there are security requirements they must abide by in Canada (PIPEDA) and the US (HIPAA) to keep client data safe.

Nonprofits that don’t comply could face thousands — if not millions — of dollars in fines.

To prevent this, here’s what your non-profit needs to know about PIPEDA, and HIPAA compliance.

WHAT IS PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA) sets the standard for how private sector organizations collect, use and disclose personal information in **Canada**.

WHO PIPEDA APPLIES TO

PIPEDA applies to all private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity. This data must be:

1. Collected with consent and for a reasonable purpose
2. Used and disclosed for the limited purpose for which it was collected
3. Accurate
4. Accessible for inspection and correction
5. Stored securely

DATA COVERED UNDER PIPEDA

Under PIPEDA, the following data is protected as sensitive or Personally Identifiable Information (PII):

- Age, name, ID numbers, income, ethnic origin, or blood type
- Opinions, evaluations, comments, social status, or disciplinary actions
- Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs)

WHAT IS HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection in the **US**.

WHO HIPAA APPLIES TO

HIPAA applies to anyone providing treatment, payment, and operations in healthcare, and anyone who has access to patient information and provides support in treatment, payment, or operations.

Other entities, such as subcontractors and any other related business associates must also be in compliance.

DATA COVERED UNDER HIPAA

HIPPA covers all protected health information (PHI), including:

- 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.

Along with this data, each patient comes with identifiers that could connect the dots between the treatment and the individuals.

HIPAA IDENTIFIERS

There are 18 traits that HIPAA looks for to identify someone:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county, zip code)
- All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89)
- Telephone number
- Fax number
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Device identifiers or serial numbers
- Web URL
- Internet Protocol (IP) address numbers
- Finger or voice prints
- Photographic images
- Any other characteristic that could uniquely identify the individual

CONSEQUENCES OF NON-COMPLIANCE

LuxSci proposed an interesting case study that proves how challenging identifying protected data and PIPEDA & HIPAA violations can be.

Let’s say a blood bank sends a newsletter offering treatment advice for recovering after donating blood. If the newsletter goes out to their entire mailing list and provides general advice for all patients, then PIPEDA & HIPAA isn’t an issue.

However, if the newsletter is sent exclusively to patients that had donated blood, then the non-profit is technically discussing past medical history that could be relevant to a doctor or something the patient is reluctant to disclose.

CONSEQUENCE OF NON-COMPLIANCE

Like most legal and insurance issues, there is plenty of grey area when it comes to punishing PIPEDA & HIPAA violators. In many cases, the judge will look at intent, knowledge, and other factors.

People tend to think about PIPEDA & HIPAA violations in a grand sense, where large amounts of patient information is stolen by a mysterious hacker-mastermind.

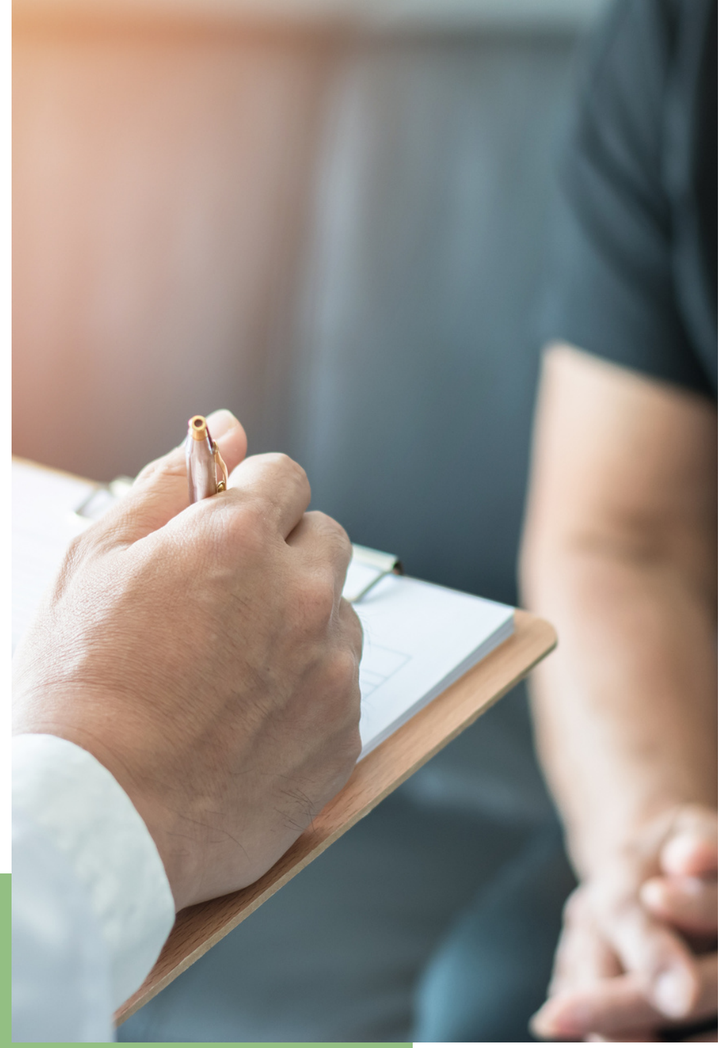
However, a PIPEDA or HIPAA violation can be as simple as sending patient records to the wrong email, or an intern taking a peek at a file they shouldn't have. In all cases, it's the role of the nonprofit to act swiftly to correct the security breach and make sure it never happens again.

CONSEQUENCE OF NON-COMPLIANCE

Organizations that knowingly violate **PIPEDA** requirements for proactive security safeguards, data breach reporting, and keeping data breach records may be fined up to $100,000 CAD per violation.

PIPEDA lists three instances that could lead to criminal prosecutions:

- Purposely destroying information after receiving a request to review that information
- Retaliatory behavior against employees who attempt to follow PIPEDA
- Hampering investigations after a complaint is lodged



CONSEQUENCE OF NON-COMPLIANCE

There are four levels of violation for **HIPAA** that a non-profit needs to be aware of.

1. The organization did not know (and by reasonable diligence could not have known) that they violated HIPAA. This leads to a minimum penalty of $100 per violation.
2. HIPAA was violated due to a reasonable cause, not due to willful neglect. This has a minimum penalty of $1,000 per violation.
3. The HIPAA violation occurred due to willful neglect, but was corrected within a required time period. This has a minimum penalty of $10,000 per violation.
4. The HIPAA violation occurred due to willful neglect and was not corrected. This has a minimum penalty of $50,000 per violation.

The maximum penalty for all four of these penalties is $50,000 per violation and an annual maximum fine of $1.5 million.

HOW SUMAC HELPS YOU BE PIPEDA & HIPAA COMPLIANT

Sumac supports all the technical requirements that enable an organization to be in compliance with the PIPEDA & HIPAA security standards, so you can rest assured knowing client data is safe. Sumac does this by:

1. Requiring passwords and user profiles that restrict visibility of the data to authorized users
2. Encrypting connections between Sumac and the database
3. Providing mechanisms for updating information in the database
4. Logging records of file access
5. Doing all the above things securely - The security required for Sumac's PA-DSS certification exceeds what the HIPAA standards require.

SUMAC
By Silent Partner

Contact our sales team today to book a free demo!

sales@sumac.com

Toll-free 1-877-399-4645