Personally Identifiable Information (PII):

A cybersecurity checklist

Personally Identifiable Information (PII) is any information or data that can be used to identify an individual. While not necessarily used within Canadian legislation like PIPEDA, it is a way to categorize information that is often collected by SMBs during business transactions or in managing clients and employees.

• A full name (not just a nickname) • Social insurance number • Home address • Location data • Home IP address • Personal email address	• Passport number • Driver's license number • Financial information • Health card number • Health information

To avoid penalties and litigation as well as reputational risk, it is important that you:

- ☐ Identify the privacy and access to information legislation and mandatory requirements for your jurisdiction. This includes understanding: ○ What PII needs to be protected?
  - ○ What are considered reasonable protections?
  - ○ What actions and reporting needs to occur in the event that PII is disclosed to unauthorized parties?
- ☐ Identify the PII you use in your business including:
  - ○ Employee information, ○ Client information, ○ Customer information or patient information, and ○ Other contact information that may be protected under law.
- ☐ Identify PII that is stored within your information systems and how it transits across your system and to others with whom you share data.
- ☐ Establish a policy within your organization that provides direction on PII handing
- ☐ Put in place sufficient cybersecurity controls to protect the PII from intentionally or accidentally being disclosed to unauthorized parties.
  ☐ Have a cybersecurity incident response plan that can kick in if there is a breach and PII security controls are potentially jeopardized.