POLICY STATEMENT:
A policy to protect Personal Health Information stored, transmitted, and transported on mobile devices by Users of the Municipality’s Public Health Department.

APPLICATION:
This policy applies to Users in the Public Health Department using technology provided by the Municipality of XXX (“the Municipality”).

PURPOSE:
The Public Health Department provides its users with business technology tools to manage business information electronically, to communicate with clients and staff, and to prepare and obtain useful business information.
This policy is designed to:

- Eliminate the risk of lost or stolen data from mobile devices;
- Ensure that the Public Health Department clients’ Personal Health Information is protected in accordance with the Personal Health Information and Protection Act, 2004; and
- Safeguard the rights of individuals whose Personal Health Information the Public Health Branch holds.

DEFINITIONS:

Encryption: The conversion of data into code for the purposes of privacy protection or security considerations.

Mobile Device: Any tool intended to store and/or distribute applications, data and configuration settings to mobile communications devices. These devices include, but are not limited to laptops, computers, USB keys (commonly referred to as memory sticks and flash drives), Portable Hard Drives, BlackBerry, Electronic Tablets, and Personal Digital Assistants (PDAs).

Personal Health Information: Identifying information about an individual that relates to his/her health.
Personal Health Information and Protection Act, 2004: Provincial legislation that, among other things, governs the collection, use and disclosure of personal health information by health information custodians.

PIN-to-PIN: A feature which supports direct messaging between BlackBerry devices.

Short Message Service (SMS): Is a communication service allowing the interchange of short text messages between Cellular Wireless Communications Devices (CWCD).

Strongly Encrypted: Having a combination of technological and functional requirements that ensures personal information is protected from access by unauthorized parties. Technological requirements include: secure implementation, secure and managed encryption keys, secure authentication of users, and no unintended creation of unencrypted data. Functional requirements include: identified, authorized and trained users, encryption by default, availability and information life cycle protection, and threat and risk assessment prior to live operations.

User(s): One that uses mobile Device(s). The term applies to any person in the Public Health Department that has been provided with mobile technology by the Municipality. It includes, but is not limited to, employees, agents, students and contractors.

REQUIREMENTS FOR USERS:

- All mobile devices must be strongly encrypted and password protected.

- When personal health information is stored on USB keys, CDs, or DVDs for transport to external agents or entities, the information must be strongly encrypted.

- When sending email communications containing personal health information external to the Region, the communications must be strongly encrypted.

- The following is prohibited in transmitting personal health information while conducting Public Health Department business:
  - Using one’s own personal mobile device;
  - Using one’s own personal email account to send emails;
  - “Text Messaging;”
  - Pin-to-Pin (commonly referred to as “PIN-ing” which is a Real-time instant-messaging-like-application); and
  - Short Message Service (SMS)
REFERENCE:

*Personal Health Information Protection Act, 2004*

CONTACT:

Privacy Officer