



## Health and Social Services

### Electronically Stored and Transferred Information Policy

---

#### Policy Statement

A consistent approach is needed to ensure safe and secure storage and transfer of electronic information.

#### Scope

This Policy applies to:

- 1) All employees, volunteers, contractors and information managers of the Department of Health and Social Services and the Health and Social Services Authorities (HSSAs) when storing and transferring personal, personal health, and confidential information in electronic format on any portable devices, including but not limited to:
  - Laptops
  - USB flash drives (USB keys, memory sticks, jump drives, thumb drives)
  - Portable external hard drives
  - Tablets (iPads, Galaxy Tab)
  - Smartphones (iPhone, BlackBerry)
  - MP3 players (iPod)
  - Electronic pen (E-pen)

#### Definitions

The following terms apply to this Policy:

"Confidential information" is non-public information that is only shared with a limited number of individuals for a specific purpose. Examples of confidential information include, but are not limited to:

- Personal information about clients (such as child protection, adoption, medical records, documents obtained for public health surveillance purposes, etc.)
- Personal information about employees (such as performance appraisals, medical notes, labour relations documentation, etc.)
- Legal opinions

- Decision papers and other material intended for Cabinet or the Financial Management Board
- Any information that, if disclosed, may result in harm to the Government of the Northwest Territories (GNWT) or other interests.

"Electronically" means anything created, recorded, transmitted or stored in digital form or in other intangible form by electronic, magnetic, optical or other similar means.

"Employee" for the purpose of this Policy means all individuals employed by the Department or HSSA including salaried, contracted or locum health practitioners and individuals whose positions are federally funded.

"Health and Social Services Authorities" or "HSSAs" refers to the Northwest Territories Health and Social Services Authority and Boards of Management under the *Hospital Insurance and Health and Social Services Administration Act*.

"Information manager" means a person or organization that provides one or more of the following services for the Department or HSSA:

- (a) the processing, storage, retrieval or disposal of personal health information,
- (b) the transforming of personal health information, including the transforming of person health information to create or produce non-identifying information, and / or
- (c) information management services, information system services or technology services.

"Personal information" means information about an identifiable individual, including

- (a) the individual's name, home or business address or home or business telephone number,
- (b) the individual's race, colour, national or ethnic origin or religious or political beliefs or associations,
- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics,
- (f) information about the individual's health and health care history, including information about a physical or mental disability,
- (g) information about the individual's educational, financial, criminal or employment history,
- (h) anyone else's opinions about the individual,
- (i) the individual's personal opinions, except where they are about someone else.

"Personal health information" means information in any form that identifies an individual, or in respect of which it is reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual:

- (a) information about the health and health care history of an individual,
- (b) information respecting health services provided to an individual,
- (c) information about eligibility or registration of an individual for a health service or related product or benefit,
- (d) information about the payment for a health service for an individual,
- (e) information collected in the course of providing a health service to an individual or information that is collected incidentally to the provision of a health service to an individual, including the individual's name and contact information,
- (f) a personal health number, other identifying number, symbol, or other particular assigned to an individual in respect of health services or health information,
- (g) prescribed information about a health service provider that provides a health service to an individual,
- (h) information respecting the donation by an individual of a body part or bodily substance,
- (i) information prescribed as personal health information in the Health Information Regulations.

"Portable devices" means any type of portable storage device that allows for the storing and transferring of information such as laptops, and USB-based removable media attached to a computer/laptop through a USB connection, such as a flash drive and external hard drive.

## **Provisions**

The following processes must be followed to protect the privacy and security of personal, personal health, and confidential information when storing and transferring information in electronic format on portable devices.

### **1) Storage**

- a) Electronically stored information must be kept in a manner that preserves its form and keeps its structure and content intact.
  - Store electronic information in its original version and avoid manipulation unless necessary.
- b) Protect electronically stored information against loss, unauthorized access, manipulation, destruction, or theft.
  - Use only secure network drives for storage.
  - Store current or frequently referenced information in a way that allows efficient and authorized access.
  - Limit access to electronic information to only those entitled to it to perform their work.
  - Local backups of electronically stored information must be performed regularly.

### **2) Transfer**

- a) Whenever personal, personal health, and confidential information is electronically transferred, it must be appropriately encrypted and/or password-protected to protect the information and prevent unauthorized access during transfer.
- b) Reusable portable devices, such as USB keys or E-pen, must be securely erased when transfer of information is complete.

**3) Portable Devices**

- a) The transfer and storage of information using a portable device must be restricted and should only be used when absolutely necessary.
- b) When information must be stored or transferred using a portable device:
  - the amount of information stored or transferred must be minimal;
  - details related to the storing or transferring of the information must be logged, including:
    - the date of the transfer to and / or storage on the device;
    - an inventory of the information being transferred and / or stored
    - the purpose of the transfer / storage, noting the reason must be 'absolutely necessary', as per the requirement under (a);
    - the individual transferring / storing the information has confirmed use of a strong password and encryption where possible for that device; and
    - the date the transferred / stored information is deleted from the device;
  - information stored must be removed as soon as possible from the device and saved onto a secure network drive; and
  - whenever possible, information transferred using a portable device should be done so over a secure network.

**4) Security**

- a) Whenever a portable device is not in use, it must be stored securely in a safe locked area (e.g. USB key in a locked cabinet).
- b) Any unattended portable device, such as a laptop, must be logged-off and automatic log-out mechanisms should always be used to prevent unauthorized access.
- c) Any unusual and suspicious events associated with electronically stored and transferred information that may lead to a privacy or security breach must be reported to the supervisor and/or Health Information Act (HIA) designated contact person.
- d) Awareness training about electronic information security (including storage, transfer and portable device use) should be maintained and regularly offered.
- e) Security standards established by the Office of the Chief Information Officer must be met.

## Authority and References

- *Access to Information and Protection of Privacy Act*
- *Electronic Transactions Act*
- *Health Information Act*
- Ministerial Directive 2017: 03 Privacy Standards, Policies and Procedures
- Privacy Breach Policy

<original signed by>

Deputy Minister

August 22, 2019

Date