eHealth Privacy Awareness

PRIVACY & SECURITY OF PERSONAL HEALTH INFORMATION IN ELECTRONIC ENVIRONMENTS

ELECTRONIC PORTAL ABRIDGED VERSION MAR 2018

"THIS IS OUR NEW CHIEF PRIVACY OFFICER...
HE TAKES HIS JOB RATHER SERIOUSLY!"

Why be ePrivacy Aware?

To ensure employees who use eHealth systems* are aware of their role and responsibility to appropriately access and use personal health information and **protect client privacy.**

To ensure employees are aware of **HSS policies and legislation governing access and use** of personal health information and client privacy.

To ensure our **clients' right to privacy.**

To qualify employees to **be eligible to use eHealth systems.**

To maintain an organization wide **privacy culture.**

To ensure employees are aware of **how to protect client privacy** and keep personal health information safe.

***Electronic health information systems**

Privacy & Confidentiality

PRIVACY is the **RIGHT of individuals** to determine when, how, and to what extent information about them is shared with others. **PRIVACY** is about protecting our client's and their information.

CONFIDENTIALITY is our legal, professional and ethical obligation, to keep information that has been entrusted to us by our clients' **PRIVATE.**
When we handle clients' information, we will only collect, access and use the **least** amount of information **needed** to do our job, and only share with individuals that **NEED TO KNOW** the information to do their job.

Privacy & Confidentiality

All personal health information is considered to be **PRIVATE.** Only specific information **NEEDED** by a health care provider to support the provision of health services to the client can be collected and used, and the health care provider must treat that information as **PRIVATE.**

A co-worker, who is **NOT** involved in a client's care and does not need the client's information to do their job, is **NOT AUTHORIZED** to request, access, or be given this information.

A family member contacts the hospital for information about a client, but the client has requested that details about their condition **NOT BE SHARED** with family members. This client's directive must be honoured; information **MUST** not be shared with the client's family members, and **MUST** be kept **PRIVATE.**

Privacy & Confidentiality

An employee who does not have access to electronic health records, asks a co-worker, who does have access, to “just look up” the personal history of the employee’s cousin, because they want to see if they share a rare medical condition…

The co-workers name is recorded in a privacy audit and, having no justification for access to the personal history of the cousin, the co-worker and the employee are both disciplined by their employer. Neither of them needed the **PRIVATE** information to do their jobs.

A test result confirming a client has a reportable disease is **PRIVATE** information, but some of this information has to be **CONFIDENTIALLY** reported to Population Health, where the information will continue to be protected and treated as **PRIVATE.**

Privacy & Confidentiality

You work as part of a clinical care team
with a Specialist and a Dietician,
to determine a care plan for your client.

This care team is permitted to **CONFIDENTIALLY** discuss pertinent medical details, but only as required to make a determination about appropriate care for the client.

All of this information is **PRIVATE.**

This information **CAN NOT be shared with others in your organization**
who do not need to know.

“Personal Health Information”

Personal Health Information (PHI), as defined by the ***NWT Health Information Act***, means the following 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.

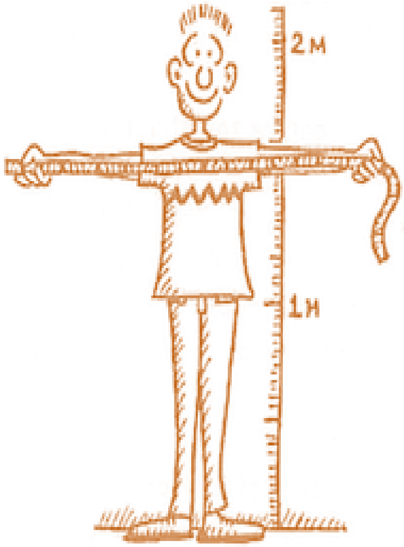
(a) information about the health and health care history of an individual;

(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;

“Personal Health Information”



(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”.

Respecting Client Privacy

Ethics/Ethical Decision Making

Even IF you can physically or electronically access a file, e.g. Lab Reports, you are **NOT ALLOWED** to view or otherwise use this file or information for just any reason…

You are **ALLOWED to access the specific information that you NEED** to provide services to a client whom you are currently and directly serving.
Such access is **AUTHORIZED.**

You are NOT ALLOWED to access personal health information that you do not need to have in order to provide services to a client for the current session of care.
This is true even if you can physically or electronically access this information.
Such access is **UNAUTHORIZED.**

Respecting Client Privacy

Ethics/Ethical Decision Making

Use the "**NEED TO KNOW**" privacy principle - Think about what specific information you will NEED in order to provide services to a specific client. **YOU** protect privacy by only accessing the **LEAST** amount of information that you need, and by **only using identifiable information when non-identifiable information will do**.

Access information when these conditions are met:

- ✓ Information is necessary for the provision of, or to assist in, the provision of a service;
- ✓ Information is necessary for making a determination for a related service;
- ✓ where the information is related to, and necessary for the current session of care.

ASK YOURSELF!

"**Do I NEED this information** to do my job?"

"**Does my co-worker NEED to know this** information to do their job?"

Respecting Client Privacy

Ethics/Ethical Decision Making

AUTHORIZED SHARING - Certain situations allow for authorized non-clinical access to personal health information, including:

- **Authorized routine disclosure -** patients requesting access to their own personal health record;
- **Disease surveillance** legislation (ref. *NWT Public Health Act*) identifies specific conditions to be reported to the Chief Public Health Officer;
- **RCMP warrant**, or a Maintenance Order;
- **Quality Assurance** Activity, etc.

AUTHORIZED ACCESS - All NWT residents have a **right to request access** to their own personal health information by formal request to their local Health Authority/Region.

Respecting Client Privacy

Unethical/ Unethical Decision Making

“PEEPING”, “SNOOPING”, “JUST LOOKING”, “SURFING”….

Accessing clients’ information without authorization is unethical and disrespects clients and clients right to privacy. “Snooping” includes looking, viewing, “surfing” or “scanning” of client information without a legitimate business reason and respecting privacy principals.

This type of use is unauthorized and demonstrates poor ethical decision making, it also shows a lack of caring, of professionalism, and of integrity, and is against HSS policy and legislation. Such use is subject to employer disciplinary process and is illegal/punishable by law.

Respecting Client Privacy

Unethical/ Unethical Decision Making

"GOSSIPING", "LOOSE LIPS", "T.M.I"...

Sharing clients' information without authorization is unethical and disrespects clients and client's right to privacy. T.M.I? = "Too Much Information!" ... and gossip or "loose-lips" is any "sharing" through any medium (manually, electronically, visually, verbally, etc.) of client's information without a legitimate business reason and respecting privacy principals.

This type of use is unauthorized and demonstrates poor ethical decision making, it also shows a lack of caring, of professionalism, and of integrity and is against HSS policy and legislation. Such use is subject to employer disciplinary process and is illegal/punishable by law.

Privacy... *in the News*

Healthcare workers breach privacy of 198 patients - *Island Health* notifying patients

June 2016 - Two Victoria healthcare workers are under investigation for accessing the electronic health records of one hundred and ninety eight Vancouver Island residents who were not under their care. The privacy breach was uncovered during a routine audit of the system, ….

The health authority…said it is notifying patients. "It is unacceptable to Island Health when our employees use their access privileges to snoop in patients' records," said the statement. "This includes unauthorized reading of a patient's chart and accessing information on yourself, children, family, friends or co-workers when the employee does not need to see or know that information to do their job." The two people involved no longer work for Island Health…

CBC News Posted: Jun 14, 2016 8:31 AM PTLast Updated: Jun 14, 2016 9:03 AM PT

Privacy… *in the News*

Healthcare workers accessing records with malicious intent…

February 18, 2015 – “One case in Alberta involved an…office clerk who was looking into the records of the wife of the man with whom [the clerk] was having an affair – the wife was also a cancer patient. In another incident, a pharmacist in a dispute with fellow… [organization member] opened their medical records to pull information about their… prescriptions and posted it on facebook. A recent high-profile Ontario privacy breach involved a health worker, who was also an activist, and who pried into more than 400 patient files, and used this information to publically target clients.

Canadian HealthCare Technology, Posted: February 18, 2015
http://www.canhealth.com/2015/02/few-provinces-report-health-data-breaches/

Photos of a dying patient posted to Facebook. Workers fired.

August 2010 – Instead of treating a 60-year-old stabbing victim after his initial arrival at St. Mary Medical Center's ER, nurses and other staff took photos of the man and posted them on facebook, the *Los Angeles Times* reports. The patient had been stabbed more than 12 times ….. His throat was sliced so severely that he was almost decapitated. He died soon after the photos were taken.

FierceHealth 2010 http://www.fiercehealthcare.com/healthcare/photos-dying-patient-posted-to-facebook-get-four-hospital-workers-fired

Privacy Safeguards

Privacy and security controls, also called "**safeguards**", serve to eliminate or reduce threats and risks to the integrity, privacy and confidentiality of information.

"Privacy Safeguards" can be:

- technical,
- physical, or
- administrative.

Think of safeguards as "**gatekeepers**" **-** they help ensure that only the right individuals gain access to the right information, helping to keep information private, confidential and safe.

Privacy Safeguards

Technical SAFEGUARDS

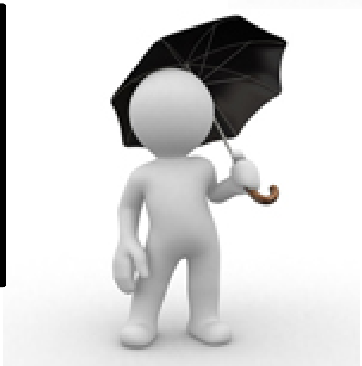
- electronic access controls (strong passwords)
- electronic audit logs and privacy auditing
- logging out of your account and computer

Physical SAFEGUARDS

- locking file drawers / high density file cabinet
- locking rooms/ buildings/ facilities when not in use
- locking docking stations or cable lock computers

Administrative SAFEGUARDS

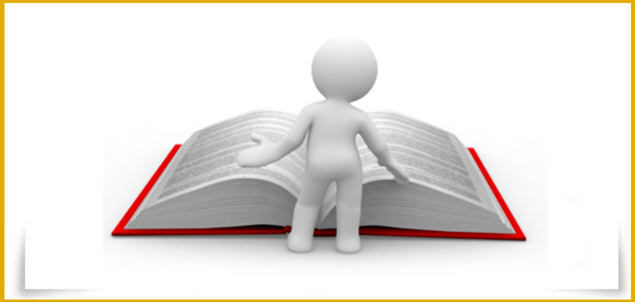
- Standard Operating Procedures
- Privacy Legislation and Policies
- Professional Codes of Conduct



Privacy Safeguards

Policies and legislation provides legal and business direction to operations and administration on appropriate protection, handling and use of personal information or personal health information:

- GNWT Acts, including :
  - **Access to Information and Protection of Privacy Act (ATIPP)**
  - **Health Information Act (HIA)**
  - Public Health Act
  - Mental Health Act
  - Vital Statistics Act
  - Electronic Transactions Act
  - Other Acts



- Health and Social Services Policies
  - Privacy Breach Policy
  - Other Policies

How to Protect Information

Protecting information depends greatly on **YOU** and **YOUR** actions**.**

Printing:

Protect information when converting into paper format:

- If available, use the "secure" or "hold" print option to prevent confidential documents being left unattended at the printer station;
- Verify your printer! **Print a generic test page first**;
- File or destroy paperwork when no longer needed and follow records management guidelines and procedures.

Viewing Information:

Protect information from accidental viewing:

- shield documents from view;
- turn monitor away from the direct line of sight;
- **install "privacy filters" on monitors**;
- revert to desktop if others come into sightline.

How to Protect Information

Speaking:
Protect information when communicating verbally:

- Only **share confidential information in a secure setting**;
- Confirm the caller's identity and only provide details that are allowed to be shared with the caller according to legislation.

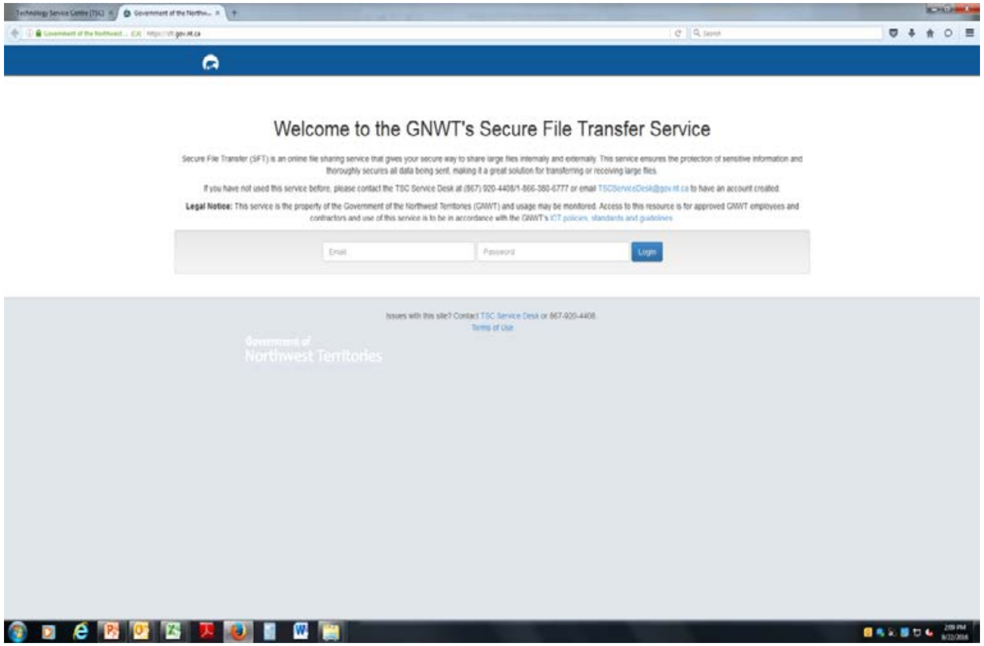
Storing and Transmitting Information Electronically:
Protect information when storing or transmitting:

- Follow policies and procedures when electronically storing, faxing and/or emailing personal health information;
- Re-confirm the recipient 's contact information before sending information electronically;
- Never take and or share screen shots of PHI;
- Use **Secure File Transfer (SFT)** option to send files electronically.

How to Protect Information

Secure File Transfer (SFT) is an online file sharing service that gives you a secure way to share large files internally and externally. This service ensures the protection of sensitive information and thoroughly secures all data being sent, making it a great solution for transferring or receiving large files"!

The GNWT Technology Service Centre (TSC) has a specific web site to access and use SFT.


Technology Service Centre (TSC)
Government of the Northw...
Government of the Northwest... (CA) https://sft.gov.nt.ca
Search

Welcome to the GNWT's Secure File Transfer Service

Secure File Transfer (SFT) is an online file sharing service that gives your secure way to share large files internally and externally. This service ensures the protection of sensitive information and thoroughly secures all data being sent, making it a great solution for transferring or receiving large files.

If you have not used this service before, please contact the TSC Service Desk at (867) 920-4408/1-866-380-6777 or email TSCServiceDesk@gov.nt.ca to have an account created.

Legal Notice: This service is the property of the Government of the Northwest Territories (GNWT) and usage may be monitored. Access to this resource is for approved GNWT employees and contractors and use of this service is to be in accordance with the GNWT's ICT policies, standards and guidelines.

Issues with this site? Contact TSC Service Desk or 867-920-4408.

How to use SFT:

- Go to http://www.tsc.gov.nt.ca/
- Click on "*Secure File Transfer*"
- Follow the instructions

Note:
Be sure to save the file to a secure location and clear your downloads folder.

How to Protect Information

USB "Rules of Thumb"
If data must be transferred via a USB, **gain appropriate approvals**, and **ensure the device is password protected**, encrypted, tracked and **secure from theft, or loss** during transfer.
Do not use for long-term storage!
Use of USB drives is highly discouraged!

Storing and Transmitting Information Electronically:

- Ensure personal health information is transmitted using approved software over **secure business networks, e.g., SFT**;
- Personal media, e.g. Facebook, @gmail, etc., **MUST NOT be used** to store, send, or receive personal health information;
- **Protect** personal health information before transmitting;
- Use **approved encryption technology -** contact the TSC or your local business IT service provider for advice on encrypting files.

How to Protect Information

Mobile Storage Devices:

- **Follow policies and procedures** when using mobile devices;
- Use only **approved**, **business** owned, mobile devices e.g. a TSC issued cell phone, USB, laptop, tablet, etc.;
- **DO NOT** use personal mobile devices, USB, cell phone, laptop etc. for business purposes;
- Do not plug personal devices into a work computer;
- Gain appropriate approvals - supervisor/management approval is required for use of business mobile devices;
- **Clear** temporarily stored health information, when not in use;
- When you leave an organization ensure you **clear and return electronic devices** including key cards, USB, laptops, phones, etc.

If you misplace an electronic device, **IMMEDIATELY** report this to your supervisor!

How to Protect Information

Opening email and web-links / Downloading Information:

- Verify the identify of the sender before opening email, web-links or attachments. Ensure mobile devices are free of malware and viruses before downloading data onto local computers, if permitted, and follow applicable policy and procedures for mobile device use.

If you suspect that an email or web-link is not safe, immediately contact the TSC (or your local IT service desk if not TSC supported).

DO NOT OPEN the email and/or any attachments!

DO tell your supervisor as soon as possible!

How to Protect Information

IS YOUR DATA SAFE? Email, Web-links and 'Downloading'

- Not everyone wants to "protect" information. **Malware** and **computer viruses** can be activated via email, web-links or downloads and can quietly **corrupt computer hard drives**, and quickly **spread to software** on other computers on the "network";
- Malware and viruses can be transferred to, or from, mobile devices;
- Data, including personal health information, stored on infected computers, servers or networks devices can be **stolen**, **temporarily encrypted, or purposefully corrupted,** so it cannot be accessed, or used, as needed for care.

How to Protect Information

Accessing eHealth Applications:

- Log out of your account and applications when not in use;
- Log out of the network and your computer when not in use;
- Lock your work station when you leave the computer temporarily;
- Do not share your username or password with anyone.

Lock your computer screen holding down the ***Ctrl + Alt + Delete*** keys and select "*lock this computer*" from the menu, or hold down the ⊞ key and type "**L**";

If your workstation has a desktop icon called "Lock your Workstation", click on the icon to lock your screen.

YOU can be held accountable if someone else gains access to a health information system and/or personal information via your account!

Password Security

- ✓ Add numbers, special characters, a mix of upper and lower case letters to add **strength** to your password (4, L, !, *, t..);
- ✓ Password length is key to **password strength:** 8 characters is minimum, 21 characters improves security;
- ✗ Do not use **date of birth, a phone number, a colour, friend's name or pet's name as your password**;
- ✗ Do not use simple combinations as your password SUCH AS "*password*", "*qwertyui*", "ABC123";
- ✗ Do not use characters in sequence or repeating characters (22222222, 12345678, abcdefgh;
- ✗ Do not write your passwords on a sticky note!
- ✗ Do not accept any electronic prompt to "save" your password, or to "remember you for next time" you log onto an application, system or network;
- ✗ **DO NOT share your password!**

STOP A "HACKER", USE A STRONG PASSWORD!

"**Hackers**" can "crack" your password , then access your computer and **steal data, files and documents.**

How to Passwords

Make your password “*work*”, and be easy for YOU to remember too!

Want to quit smoking, be more active, save money towards a new truck? **Your password can help!**

It’s simple to remember your password when you relate it to a personal goal such as: “**my*NewFordTruck*2017***”

This way, you will remind yourself of your goal AND recommit to your goal every time you type in your password! Achieved your goal? Just change your password, to a new goal? Now, all you have to remember is to **keep your password secret – it’s that easy!**

Privacy/Security Risks & Incidents

WHY CAN'T I LOOK AT MY OWN RECORD!?!

Accessing your own or your parent's, sibling's, child's spouse's, other family member's, or any other record you have no need to access is…

- **UNAUTHORIZED** and is a violation of both the Terms of Use for information systems, and NWT Legislation;
- **UNETHICAL** and contrary to professional practice and of client obligation;
- **AN ABUSE** of position and of a position of power, and;
- **UNDERMINES the PRINCIPLE OF EQUAL ACCESS** to health services for all NWT residents;
- May **EXPOSE** clients to **INFORMATION** they would not otherwise be permitted access to, and **MAY CAUSE HARM**;
- Presents an **OPPORTUNITY FOR DATA TAMPERING/ COMPROMISES THE INTEGRITY OF INFORMATION** that service providers rely on to make an accurate determination about treatment and services required by clients.

Privacy/Security Risks & Incidents

Examples of Risks and Incidents:

- **CONDUCTING OR PERMITTING unauthorized access, collection, use or disclosure of personal health information**;
- Unauthorized disposal, destruction, alteration of information.
- Unauthorized access to hardware or software:
- Allowing others to use your electronic account after you log on;
- Using someone else's username, or password;
- Sharing your username and password;
- **GATHERING, ACCESSING, CHANGING (edit), or otherwise USING INFORMATION (snooping)** that is not needed for you to perform your business function/job duties related to the provision of health services to a client;
- **Discussing/disclosing client information to people who do NOT NEED TO KNOW**, internal/external to NWT HSS (any media or means of communication at work, at home, in public, at play, in transport, on-line, telecom., verbal, written, any signal, any code).

Privacy/Security Risks & Incidents

Don't risk your future!

Consequences for violating client privacy and electronic system security may increase based on the nature of the breach!

- Electronic system **accounts** may be **suspended**;
- Employers may **discipline** or **cancel work contract**;
- **Fines ($)** may be levied under ATIPP and/or HIA*;
- Professional bodies may fine or **revoke licensing**;
- Clients or families may take **legal action**.

** An individual employee can be fined $50,000 per offence, under the NWT HIA.*

Incident Handling 101

RULE #1:

- ✓ BE CALM and DON'T PANIC!!

RULE #2:

- ✓ PROTECT INFORMATION AND CLIENT PRIVACY!
- ✓ RECOGNIZE RISKS and PROCEED WITH CAUTION
- ✓ FOLLOW POLICY AND PROCEDURES (SOPs)
- ✓ REPORT INCIDENT TO YOUR SUPERVISOR

Summary – Your Privacy Mantra

As a client I have a right …

… to request access to my personal health information!

….to privacy.

… to set limits on collection, use and sharing of my information.

Summary

“I understand and follow policies, guidelines, professional codes of conduct…

…and best practices to protect the privacy and security of information”.

Summary

"I ensure information is handled and stored securely!"

"I access only the information I NEED TO KNOW to do my job!"

"I use strong passwords, AND don't share my password."

Summary

“I do not access or use my own or family members’ information!”

“I report suspected risks to privacy or security of information!”

“I don’t talk about or share clients’ information that others don’t NEED TO KNOW.”

Summary

"I don't open or click on suspicious emails or web-links!"

"I always log-on to my own account and log-off when my session is done!"

"I don't store or download personal documents on work devices/ computers!"

eHealth Privacy Awareness

TAKE THE E-HEALTH PRIVACY QUIZ

1. FOLLOW INSTRUCTION TO COMPLETE THE QUIZ.
2. COMPLETE THE QUIZ.
3. SUBMIT THE QUIZ TO THE TRAINER OR YOUR MANAGER.

"THIS IS OUR NEW CHIEF PRIVACY OFFICER... HE TAKES HIS JOB RATHER SERIOUSLY!"