PROGRAM Standard Operating Procedure	
Title: Printing Sensitive Information	Policy Number: 28-06-V1
Program Name: Privacy and Confidentiality	
Applicable Domain: Risk and Compliance Services	
Additional Domain(s): Administration and Leadership	
Effective Date: 15/02/2024	Next Review Date: 14/02/2027
Issuing Authority: NTHSSA CEO	Date Approved: 14/02/2024
Accreditation Canada Applicable Standard: Service Excellence 3.9,6.3,7.2,7.3,5.6,7.3,9.5,9.6, Leadership 1.5, 11.2,11.3, 15.4,15.5,15.6.	
Accrediting Body and Standard: NA	

GUIDING PRINCIPLE:

The Northwest Territories Health and Social Services Authority (NTHSSA) embraces a culture where all staff and leadership are committed to protecting the privacy and maintaining the confidentiality of our clients, staff, and community members.

The NTHSSA is committed to preventing the occurrence of privacy breach incidents arising from erroneous printing of sensitive information. This SOP is to ensure public trust in the health care system and to improve the overall quality of care.

PURPOSE/RATIONALE:

To provide clear direction to all NTHSSA staff on processes to follow when printing documents containing confidential information. This Standard Operating Procedure (SOP) details four (4) approaches that, if followed, will abate the occurrence of privacy breaches resulting from misdirection of print documents and unauthorized disclosure of clients' sensitive information.

DEFINITIONS:

ATIPP refers to the *Access to Information and Protection of Privacy* (ATIPP) Act (the Act) which applies to protect individual’s privacy by governing the collection, use, sharing and storage of personal information. The *Act* recognizes an individual’s right to access and/or correct their own information.

HIA refers to the *Health Information Act* (HIA) which was passed in March 2014 that protects client’s privacy by governing the collection, use, sharing and storage of their personal health information. The *Act* recognizes an individuals’ rights to access their own information and the need of health service providers to collect, use and share client information to provide the best care possible.

Privacy Breach is defined as access, collection, use or disclosure of personal information, health-related or otherwise, whether accidental or deliberate, that is not authorized by the *Health Information Act (HIA)* or the *Access to Information and Protection of Privacy (ATIPP) Regulations*.

Sensitive/confidential information means information including personal information and / or personal health information defined and protected by the Health *Information Act (HIA)* or the *Access to Information and Protection of Privacy (ATIPP) Act*.

Unauthorized access occurs when individuals have access to personal information or personal health information they are not authorized to view, either intentionally or unintentionally.

Unauthorized disclosure occurs when personal information or personal health information is released or revealed by any means, whether accidental or deliberate, that is not authorized by the *Health Information Act (HIA)* or the *Access to Information and Protection of Privacy (ATIPP) Act.*

SCOPE/APPLICABILITY:

This SOP applies to all NTHSSA employees and other persons acting on behalf of NTHSSA (including contracted service providers) who print documents containing clients' confidential personal and / or personal health information.

PROCEDURE:

The below privacy best practices must be utilized to prevent errors and protect privacy when printing confidential information:

1. **Preprogram Printer Settings to limit print options.**

   Ensure to pre-program your workstation to limit printer options available for selection when printing documents.

   - Each workstation should have a limited number of printers e.g., one or two, to limit selected printer options.

- If your workstation has unlimited or no pre-programmed printers, contact the Technology Service Center (TSC).
  - Where a workstation cannot be pre-programmed with printer options, managers should ensure that the correct printer has been selected as the default printer on such workstations.
  - Managers should communicate with staff that altering printer settings in any situation without prior permission or authorization is prohibited.

2. **Apply Pre-print Checklist to verify printer before hitting the 'print' button.**

Printing 'test' document: Create a word document containing "test" as a test document to the printer you intend to print. Physically check the printer feed to verify that your test document has been printed at the intended printer.

- If your verification is successful, you can print confidential information from your workstation on that printer if you are certain that the print setting cannot or has not been altered since you printed the 'test' document.

- If your verification is unsuccessful, attempt to understand where the 'test' document was printed. Then, physically verify the name of the printer you intend to print on (NTHSSA printers have the printer names labelled on the printer or ask for help if you cannot find the printer's name).

- Having noted the intended printers name, verify that the name of the printer is the same name that appears in the computer printer settings and select the printer as your new 'default' printer.

- If you still cannot print to the desired printer, ask your supervisor for help or contact TSC. If another printer is in your proximity, you might select the printer and start over, beginning with printing a 'test' document.

It is important for all employees to re-verify the printer that a workstation is sending documents to after any physical installation of a new computer or printer; repair and / or reinstallation of an existing computer or printer, and/or after any network or local end point re-configuration or upgrade.

- The printer settings should be re-verified if a temporary worker/ casual employee and or locum physicians returning had been using a workstation as they may have changed the settings to use above approach.

3. Use 'Secure Print' Setting

All centrally located NTHSSA shared printers have a printing option called "secure print"; most newer model printers, especially multifunction printers have this feature. Secure print allows for the use of a pre-setup passcode to be entered on the printer prior to the machine printing sent document(s). When using secure print, documents sent to the printer do not print, but instead queue automatically until the user physically goes to the printer, enters their pre-set passcode on the printer, and selects print.

The secure print feature allows documents to be printed only when the user is physically present at the printer and hence observes the printing of the documents in real-time. This prevents unauthorized access to printed confidential documents in two (2) ways:

i. If the documents are sent to the desired printer, confidential documents are not left unattended at the printer.
ii. If the documents are erroneously sent to the wrong printer (e.g in the same or another building), the documents will not print out and the risk of anyone accidentally viewing the documents is eliminated.

When using the secure print function, it is important to de-identify the title of the document to be printed by ensuring that it does not to include any personal or personal health information. This is because the document title will be visible in the electronic display window of the printer; and anyone who views the print queue list will have access to the document title.

To set up secure print on your workstation, please refer to Appendix A - Information *Services Secure Print Guide,* dated *August 2021.*

4. Preconfigure user ID Cover Page to prevent access by others.

This involves the printing of a cover sheet with whatever print jobs are sent to a printer. Users can have their workstations configured to always print a cover sheet with each document they print.

The cover sheet distinguishes the document from other printed documents on the printer tray to prevent others from seeing what was printed should they pick up printed documents from the printer.

This approach should only be used when secure print feature is not available on a printer and should only be used in combination with approach 1 and 2 above.

If you require help with setting up your workstation for automated cover sheet printing, contact TSC for further assistance.

Disclaimer Message: This is a **CONTROLLED** document for internal use only. Any documents appearing in paper form are not controlled and should be checked against the electronic file version prior to use.

PERFORMANCE MEASURES:

RL6 incident reports will be monitored by the Unit Managers and the Risk Manager for incidents indicating non-compliance with this policy and procedures.

CROSS-REFERENCES:

NA

Attachments:

Appendix A – Information Services- Secure Print Guide- August 2021.

Appendix B – Practice Secure Printing Poster

REFERENCES:

Government of the Northwest Territories (GNWT). (2017). Department of Health and Social Services. Privacy Breach Policy

Government of the Northwest Territories (GNWT). (2020). Department of Justice. Access to information and protection of privacy act. Retrieved January 26, 2023, from https://www.justice.gov.nt.ca/en/files/legislation/access-to-information-and-protection-of-privacy/access-to-information-and-protection-of-privacy.a.pdf

Government of the Northwest Territories (GNWT). (2020). Department of Justice. Health information act. Retrieved January 26, 2023, from https://www.justice.gov.nt.ca/en/files/legislation/health-information/health-information.a.pdf

Disclaimer Message: This is a **CONTROLLED** document for internal use only. Any documents appearing in paper form are not controlled and should be checked against the electronic file version prior to use.

APPROVAL:

T. V.

Executive Director, Corporate and Support Services

February 14, 2024

Date

APPROVAL:

Joanne

Executive Director, Clinical Integration

February 12, 2024

Date

Secure Print

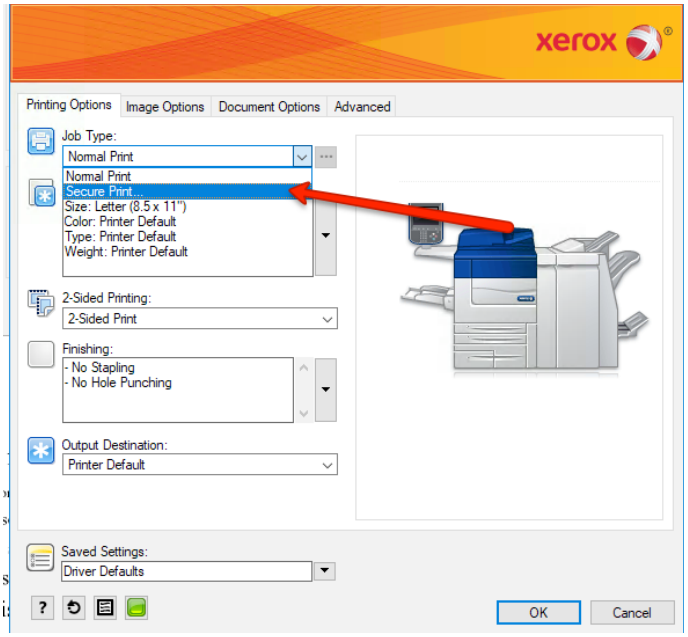
If you have questions about the privacy compliance, legislation, training, privacy of personal and/or health information, please contact the DHSS Health Privacy Unit.

WHAT: Protect the Privacy of Personal and/or Health Information

WHY: ***Secure Print*** allows you to control printing document(s), ensures document(s) is handled only by authorized staff.

HOW: Use the "***Secure Print*"** function, available on most multifunction printers, when you require securely print document(s) that contain personal and/or health information.

STEP 1: Open the **Printer Properties**, found when you open the Print function. Select **Secure Print** from the drop down list.



Job Type: Normal Print

Normal Print
Secure Print...

Size: Letter (8.5 x 11")
Color: Printer Default
Type: Printer Default
Weight: Printer Default

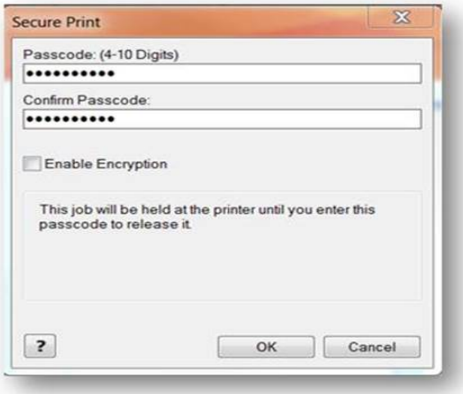
2-Sided Printing: 2-Sided Print

Finishing:
- No Stapling
- No Hole Punching

Output Destination: Printer Default

Saved Settings: Driver Defaults

STEP 2: The **Secure Print Setup** window will open**.** Choose a **4-10 digit numeric passcode** and enter it twice. Click **OK** to close the Secure Print window.



Passcode: (4-10 Digits) ••••••••••

Confirm Passcode: ••••••••••

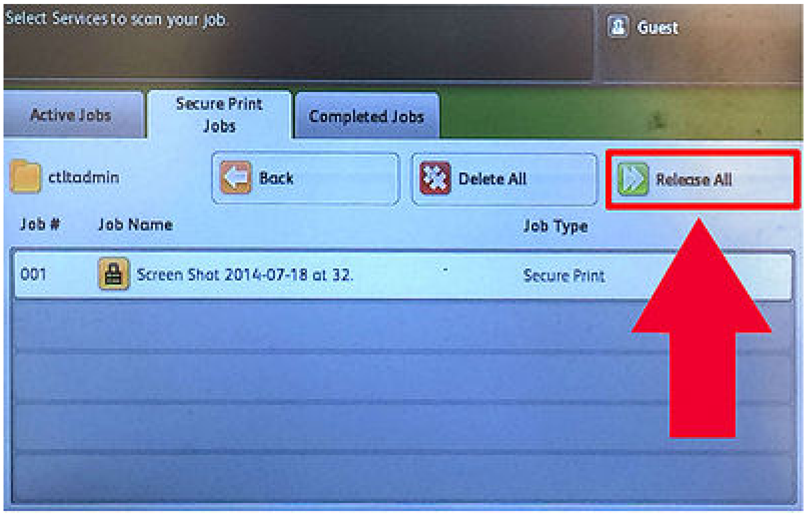
□ Enable Encryption

This job will be held at the printer until you enter this passcode to release it.

STEP 3: Click **OK** to close the Printing Preferences window.
STEP 4: Click **OK** to close the Printing Properties window.

When you print a document, it will be **held in the printer's queue until you visit the printer** and release the job with your chosen Secure Print password. Follow these instructions to release the job:

<u>At the printer:</u>



Job #	Job Name	Job Type
001	Screen Shot 2014-07-18 at 32.	Secure Print

STEP 1: Press the **Job Status** button on the printer
STEP 2: Select your document by pressing its line on the copier screen
STEP 3: Press the **Release** button on the copier screen.
STEP 4: Enter your **Secure Print** passcode using the copier keypad and press **Enter** on the screen.
STEP 5: The document should be printing.

PRACTICE SAFE PRINTING

Privacy breaches can occur when printing personal health information or confidential information to the wrong printer. The most common cause is human error.

How YOU can prevent breaches:

1. Pause before printing:

- Does the document contain sensitive personal information or confidential personal health information?
- What is the impact if the information is read by the wrong person?
- What can you do to prevent a privacy breach from occurring?

2. Consider the best options:

- Use secure print when printing confidential personal health information (Ask your local IT for information/to set up)
- Send a test page
- Use the default printer if you know it is the right location
- Only use Quick Print if you know where it prints
- Purchase a printer for your workspace if frequently printing confidential documents

3. Double check:

- The document you're printing
- The printer option & location
- Take note of the printer prior to hitting print
- Ensure that all confidential documents are not left unattended or left in the exit tray
- Ensure you collected your own documents only and not another person's document(s) by mistake

***Note:** Everything printed, copied, faxed, or scanned is stored on the printer hard drive which could be used to monitor printer misuse and inappropriate access to sensitive information.*

NTHSSA • ASTNO

Documents containing Personal Information that are found unsecured will constitute a privacy breach, which will requires employees to retrieve, secure and report the incident to the Territorial Risk Manager.