University Health Network
Policy & Procedure Manual
Administrative – Storage, Transport & Destruction of Confidential Information

Policy

At University Health Network (UHN), paper and electronic records containing personal health information (PHI) and corporate confidential information (CCI) are protected to ensure patient privacy and Hospital integrity.

To protect confidential information throughout its lifecycle (i.e. from the time it is created or collected to the time it is irreversibly destroyed), UHN employs different types of safeguards appropriate for each type of format/medium in which the information is saved. Records containing PHI receive the highest level of protection, as required by law, and must be protected using the procedures herein. Staff must use their discretion when storing, transporting and destroying records containing CCI to ensure that information is appropriately protected.

Confidential information, including PHI and CCI, must be retained in accordance with UHN Medical Record of Personal Health Information policy 1.40.009, and Management, Retention & Disposal of Administrative Records policy 1.30.007.

PHI must be stored securely according to the Storage of Information at Rest procedures herein.

Access to PHI must be restricted to those who require the information to fulfill their job duties. (See Privacy policy 1.40.007 and UHN Medical Record of Personal Health Information policy 1.40.009 for more details.)

Removal of PHI from UHN premises and/or networks is prohibited except when in transit between UHN locations or, when necessary, for the execution of job duties and, in either case, only where the information is appropriately safeguarded, as described in Transporting Information outside UHN Premises/Networks.

Once materials containing PHI have been appropriately identified for disposal, the materials must be irreversibly destroyed to the degree that the information contained therein is unrecognizable and cannot be reconstructed.

Responsibilities

All personnel and departments at all UHN sites are responsible for ensuring that the storage, transportation, and destruction of all confidential materials in their possession are done in accordance with this policy. The Privacy Office must be contacted at 416-

340-4800 ext. 6937 (14-6937) or at privacy@uhn.ca if staff discover confidential material or waste which is not stored, transported or destroyed in a secure fashion.

Certificates of Destruction must be provided by **third-party vendors** to the appropriate UHN manager, on a timely basis, for retention on file for the period prescribed in Management, Retention & Disposal of Administrative Records policy 1.30.007. In the event that the vendor is temporarily unable to provide service, the department that handles internal waste will securely store the materials on-site until service resumes. If the delay is significant, a new vendor will be procured or the contract renegotiated.

Failure to comply with this policy may result in disciplinary action up to and including termination.

Third-party Vendors

All vendors hired by UHN to store, transport or destroy confidential materials must be bonded and insured with a commitment to confidentiality and the methods documented in the vendor contract.

Storage and destruction vendors will be selected on the basis of their ability to comply with the following elements, which must be specified in the contract, namely, that the vendor:

- has written policies and procedures that specify how material will be safeguarded;
- has indemnification coverage for contractual liabilities accepted;
- requires personnel to sign confidentiality agreements;
- trains personnel on policies and procedures;
- securely transports and stores materials prior to destruction or long-term storage;
- provides a Certificate of Destruction for each destruction event;
- destroys materials using methods identified by the CIO and/or Privacy Office;
- submits to requests by UHN to witness internal processes and/or audit compliance with the contract; and
- where possible, recycles destroyed material in compliance with the Ontario Electronic Stewardship and/or Basel Action Network standards.

Vendors hired to destroy confidential materials must provide a Certificate of Destruction to the department responsible and a copy to the Manager of Health Record Services, confirming the destruction of the material provided. (Refer to Management, Retention & Disposal of Administrative Records policy 1.30.007 for the retention period.) The Certificate of Destruction must contain, at minimum:

- vendor name

- order number
- type of material destroyed
- quantity of material destroyed (volume, number, weight, or list of identifiers {Medical Record Number(MRN), Patient name, Visit number} as appropriate)
- time, date and location of the destruction
- method of destruction
- compliance with the contract and/or terms and conditions
- name and signature of the operator who performed the destruction

See Appendix A for an example of a Certificate of Destruction.

Definitions

Corporate confidential information (CCI): Information maintained by UHN that is not routinely made publicly available, including financial, administrative, commercial and technical information, and can also include records containing legal advice and employee-related information. These records may be subject to the Freedom of Information and Protection of Privacy Act (FIPPA).

Medical device: (As defined in the Canadian Food & Drugs Act and the Canadian Medical Devices Regulations.) An article, instrument, apparatus or contrivance, including a component, part or accessory of one, that is manufactured, sold or represented for use in the:

- diagnosis, treatment, mitigation or prevention of a disease, disorder or abnormal physical state, or its symptoms, in a human being;
- restoration, correction or modification of a body function or the body structure of a human being;
- diagnosis of pregnancy in a human being; or
- care of a human being during pregnancy, and at and after the birth of a child, including the care of the child.

Personal health information (PHI): Any identifying information about an individual relating to the individual's health or to the provision of health care to the individual. For example, an individual's health number and/or medical record would be considered personal health information, subject to the Personal Health Information Protection Act (PHIPA).

UHN premises: Any location where care is provided or business is conducted on behalf of UHN, including main sites (Toronto General Hospital, Princess Margaret Cancer Centre, Toronto Western Hospital, Toronto Rehab Institute), research facilities, administrative offices and other off site/satellite locations.

Procedures

Storage of Information at Rest (i.e. not in transit)

Paper

1. Store paper containing PHI on the UHN premises at which it was collected or created unless:

    - transfer to another UHN premises has been approved for patient care or another business purpose, or
    - transfer to a contracted storage vendor is required for long-term storage.

2. Store paper in a locked cabinet, container, and/or room, whose access is restricted to the individuals who require the information to fulfill their job duties or provide service (e.g. long-term storage).

3. Transfer contents to electronic form whenever possible and apply safeguards as in Electronic Files.

4. Clearly separate and mark materials that are being stored for pick-up for secure destruction.

Electronic Files

1. Store electronic files containing PHI on a secure UHN network, except when:

    - transportation or storage onto a device is required to provide patient care or complete another business purpose and access to a network is unavailable, and
    - the device is **encrypted**.

    Note: Tools or software requiring hard drive storage for patient care functions must be reported to Information Security at iso@uhn.ca. Where PHI is saved to a medical device and it is not possible to encrypt the device, the device will be physically secured to reduce the risk of theft and loss.

2. Restrict access to electronic files by:

    - Restricting access to shared network drives or folders within a drive.

    - Password protecting files and communicating the password to limited individuals.

Transporting Information outside UHN Premises/Networks

1. Only remove paper or electronic devices/media containing PHI from UHN premises and/or make copies of PHI saved to a UHN network in the following limited circumstances:

    - the information is **necessary** to complete job duties in a timely manner, including, but not limited to:

        a. transporting materials between UHN sites
        b. taking PHI into the community or collecting PHI in the community during the course of providing care, or
        c. transporting materials to a storage or destruction facility
        d. another authorized purpose

    - only **copies** of the information are removed (unless transporting for the purpose of long-term storage or destruction)
    - only the **minimum amount of information** needed to complete the task is copied or collected
    - materials remain in the **possession** of the individual at all times, unless a contracted or reputable service is used for transportation (e.g. storage or destruction vendor; Canada Post; courier)
    - information is **de-identified** prior to copying or at the time of collection or, if de-identification is not possible, electronic devices (e.g. laptop) or media (e.g. USB key) on which information is stored are **encrypted** using software/tools approved by the chief information officer and protected with sufficiently complex passwords
    - information is only removed for the **minimum amount of time** necessary to complete the task
    - information stored on **paper** is returned to UHN and **removed** from electronic devices and media as soon as no longer needed

2. Secure materials (paper, devices and/or media) when removing from UHN premises/networks by using appropriate safeguards, including:

    - taking the most direct route to the destination and avoiding stops in transit
    - transporting materials in a secure/closed container or locked vehicle (i.e. if transporting in a car, lock them in the trunk) or on one's person
    - being discreet when in transit or public to avoid drawing attention to the materials (e.g. concealing a device in an unmarked bag or container, avoiding use in public)
    - never leaving materials unattended in public areas or transport vehicles (i.e. remove from vehicle as soon as possible)
    - restricting access to materials when off-site (e.g. locking devices in a cabinet or taking other steps to limit access by unauthorized individuals)

Note: Sending PHI to an offsite recipient using Canada Post or a courier service is acceptable.

Destruction

1. Use UHN Medical Record of Personal Health Information policy 1.40.009 and Management, Retention & Disposal of Administrative Records policy 1.30.007 to identify which materials must be retained and which materials may be destroyed.

2. Securely store materials identified for destruction following the procedures in Storage of Information at Rest until destroyed or handed off to a designated destruction vendor.

3. The log and Request to Destroy Personal Health Information and Validation of Destruction (Appendix A) will be signed and dated by the director of the program responsible for destroying the records and by the manager of Health Information Management, or designate.

4. Use the **appropriate method** for destroying materials containing PHI.

Material	**Appropriate Method of Destruction***	**Procedure**
Paper (e.g. printouts, faxes, letters, labels, etc.)	Cross or micro cut shredding	Cross/micro cut, shred or place in vendor-provided shredding consoles
CDs, DVDs, disks, USB keys	Shredding or breaking into pieces	Shred or place in vendor-provided shredding consoles
Blue cards or armbands	Shredding	Shred or place in vendor-provided shredding consoles
Audio or video tapes	Shredding	Shred or place in vendor-provided shredding consoles
Pictures, slides	Shredding	Shred or place in vendor-provided shredding consoles
Medication containers (bottles and bags) with ID labels	Shredding of container or incinerating with pharmaceutical waste	Return containers to supplier along with unused medications (e.g. in Pyxis or Pharmacy cassettes or return bins)
IV bags	Shredding of label with paper (see above)	Remove label and shred or place in vendor-provided shredding consoles (place bag in garbage)
X-ray film	Shredding or silver recovery/removal	Place in vendor-provided console
Electronic devices with memory storage (e.g. laptops, PCs, printers, Dictaphones)	Data wiping prior to redeployment (according to NIST SP800-88 and ISO 27002 standards for media	With an asset tag: Call Service Desk

Material	Appropriate Method of Destruction*	Procedure
	sanitization). Degaussing, sanitization or physical destruction of storage components (shredding, snapping, drilling, incinerating or pulverizing) prior to disposal	
	Degaussing, sanitization or physical destruction of storage components (shredding, snapping, drilling, incinerating or pulverizing) prior to disposal	Without an asset tag: Call Housekeeping/Transportation for pick up

***** Appropriate methods will be tailored according to legal requirements and industry best practices (e.g. resulting particle size for shredded paper) and will be specified in agreements with waste vendors. Recycling is not an appropriate method of destruction for material containing confidential information, including PHI.

References

1. Personal Health Information and Protection Act, 2004
2. Public Hospitals Act, R.R.O. 1990, REGULATION 965
3. The College of Physicians and Surgeons of Ontario, Policy # 4-12, Medical Records

Appendix A: Request to Destroy Personal Health Information and Validation of Destruction

Log and Request to Destroy Personal Health Information & Validation of Destruction

Date:_____

Service Provider:_____

Log of Records for Destruction
(must include the names of the patients to whom the records of personal health information refer; the Medical Record Number, the date and manner of destructions). (The log can be electronic or hard copy.)

_____

_____

Approval of Program Director:

_____

Approval by Manager, Health Information Management/or Designate:

_____

Dear Service Provider:

To ensure the privacy of records containing any personal health information, please complete the required information below to validate the destruction of the records identified above.

_____validates that the above named records
Company name

have been received from _____, University Health Network
Program/department

and have been destroyed by_____.
Preferred method of destruction: fine shredding/silver recovery, incineration

_____

Signed by _____, _____
Please print name Signature

Signed by _____, _____ at _____
Signature Please print name Time

this _____ day of _____ 20_____.
Date Month Year

Please retain a copy for your files.