MUSKOKA ALGONQUIN HEALTHCARE	**Policy/Procedure Name:**	**Storage, Transport & Destruction of Confidential Information**
Manual: Administration	**Number:**	
Section: Risk Management	**Effective Date:**	01 Dec 2012
Pages: 1 of 8	**Revision Date:**	

Purpose

The purpose of this policy is to establish the standards for the proper disposal of Confidential and/or Sensitive Information (including, but not limited to, Personal Health Information (PHI)).

Scope

The policy pertains to all staff members and physicians at Muskoka Algonquin Healthcare (MAHC).

Policy Statement

At Muskoka Algonquin Healthcare (MAHC), 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 (from the time it is created or collected to the time it is irreversibly destroyed), MAHC 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. To protect CCI to the highest degree, use the procedures herein for storing, transporting and destroying PHI.

Confidential information, including PHI and CCI, must be retained in accordance with the MAHC Health Records and Chart Completion policy and the Records Retention and Destruction policy. 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. Removal of PHI from MAHC premises and/or networks is prohibited except when in transit between MAHC locations or, when necessary, for the execution of job duties and, in either case, only where the information is appropriately safeguarded, as described below in Transporting Information Outside MAHC 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.

Definitions

Corporate confidential information (CCI) – Information used for MAHC management, business or financial purposes, including, but not limited to:

- information on salaries and benefits
- information on Hospital payments such as OHIP numbers
- information on Hospital budgets, expenses or planning
- patient health information or other data used by administration/management for logging, registering, scheduling, tracking, or billing patients
- sensitive or privileged legal information
- employee status information/communications regarding any employee □□information that could expose the organization's reputation to damage □□information regarding use of animals at MAHC for research □□information regarding use of compounds or devices that could expose internal MAHC operation to malicious acts by external parties (e.g., use of a compound or device that would signal to an activist group that certain types of experimentation are being carried out at MAHC)

Personal health information (PHI) – Information about an individual whether living or deceased and whether in oral or recorded form. It is information that can identify an individual and that relates to matters such as the individual's physical or mental health, the providing of health care to the individual, payments or eligibility for health care in respect of the individual, the donation by the individual of a body part or bodily substance and the individual's health number (Personal Health Information Protection Act, 2004, section 4.1 at http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm.)
Personal health information can be information about a physician or other care provider, a hospital staff person, a patient, or a patient's family member. Examples of personal health information include, but are not limited to, a name, medical record number, health insurance number, address, telephone number, and personal health information related to a patient's care such as test results, treatment and medication records, blood type, X-rays, or consultation notes. Research related information such as research study participation, test results, or sample data are also personal health information. Personal health information includes all that is written, verbal, in hard copy, on microfilm, scanned, photographed, in computerized or any machine-readable form and electronically stored or transmitted (includes the medical record, clinical and non-clinical data).

Personal information is recorded information about an identifiable individual including:

- the individual's address, telephone number, fingerprints or blood type,
- information about the individual's race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status,
- information about the individual's educational, medical, psychological, criminal, or employment history or information concerning his or her financial transactions,
- any identifying number, symbol or other particular assigned to the individual,
- the individual's personal opinions or views except when they relate to someone else,
- private or confidential correspondence sent to an institution by the individual, and replies to that correspondence that would reveal the contents of the original correspondence,
- the views or opinions of someone else about the individual, and

- the individual's name when it appears with other personal information about that individual or when disclosure of the name would reveal other personal information about that individual.

Identifying information is information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

Medical device (Canadian Food & Drugs Act and the Canadian Medical Devices Regulations definition) – 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.

MAHC premises is any location where care is provided or business conducted on behalf of MAHC, including main Hospital sites (Huntsville District Memorial and South Muskoka Memorial Hospital) and other off site/satellite locations.

Responsibilities

In consultation with ICT management, the Privacy Officer is responsible for identifying and communicating the requirements and best practices for the storage, transportation and destruction of confidential information to appropriate MAHC groups for implementation (including but not limited to IM/IT teams, facilities management).

ICT management is responsible for identifying current best practices to secure electronic devices and media.

The Privacy Officer is responsible for educating personnel on employing specific technologies or tools to safeguard information during storage, transportation and destruction.
All personnel and departments at all MAHC 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 Officer must be contacted at ext. 6001 if staff discovers confidential material or waste is not stored, transported or destroyed in a secure fashion.
Certificates of Destruction must be provided by third-party vendors (if vendor is not on contract) to the appropriate MAHC manager, on a timely basis, for retention on file for the period

prescribed in the Records Retention and Destruction Policy. Failure to comply with this policy may result in disciplinary action up to and including termination.

Third-party Vendors

All vendors hired by MAHC 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, where not covered by the contractual agreement;
- destroys materials using methods approved by ICT management and/or Privacy Office;
- submits to requests by MAHC 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, which confirms the destruction of the material provided and contains, at minimum:
    - vendor name
    - order number
    - type of material destroyed
    - quantity of material destroyed (volume, number, weight, or list of identifiers 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

Procedure

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

Paper

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

- transfer to another MAHC 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 MAHC 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 the MAHC Privacy Office. 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.
   -

<u>Transporting Information Outside MAHC Premises/Networks</u>

1. Only remove paper or electronic devices/media containing PHI from MAHC premises and/or make copies of PHI saved to a MAHC 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 MAHC 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 ICT management and protected with sufficiently complex passwords,
- information is only removed for the **minimum amount of time** necessary to complete the task, and
- information stored on paper is **returned** to MAHC and **removed** from electronic devices and media as soon as no longer needed

2. Secure materials (paper, devices and/or media) when removing from MAHC 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 (i.e., in BlackBerry holster).
    - 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 off site recipient using Canada Post or a courier service is acceptable.

Destruction

1. Use the MAHC Health Record and Chart Completion policy and the Records Retention and Destruction policy 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. Use the **appropriate method** for destroying materials containing PHI.

Material	Appropriate Method of Destruction*	Procedure**
Paper (e.g. printouts, faxe, letters, labels etc.)	Cross or micro shredding	Cross/micro cut shred or place in vendor-provided shredding consoles
CD's DVD's, disks, USB keys	Shredding or breaking into pieces	Electronic formatting if possible then shred or place in vendor provided shredding consoles
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
IV bags	Shredding of label with paper (see above)	
X-ray film	Shredding or silver recovery/removal	
Electronic devices with memory storage (e.g. laptops, PC's, printers etc)	Data wiping prior to redeployment (according to NIST SP800-88 and ISO 27002 standards for media sanitation). Degaussing, sanitization or physical destruction of storage components (shredding, snapping. Drilling, incinerating or pulverizing) prior to disposal	Call ICT

*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.

**If purchasing a shredder, contact the Privacy Office for latest best practice for resulting particle size.

Return Upon Termination

Upon termination of affiliation with MAHC, the individual's manager ensures that:

1. Responsibility for all databases of PHI is transferred to current personnel.
2. All materials (paper, devices, and media) that are the property of MAHC and/or contain PHI for which MAHC has custody are returned to the Hospital.
3. The individual has deleted any PHI from personal systems and/or has securely wiped and/or physically destroyed devices and material prior to disposal.

Cross Reference

Health Records and Chart Completion policy

Records Retention and Destruction

Notes