



	Policy/Procedure Name:	Portable Devices and Media
Manual: Administration	Number:	
Section: Risk Management	Effective Date: 01 Dec 2012	
Pages: 1 of 4	Revision Date:	

Purpose

To ensure confidential corporate information is protected to maintain the confidentiality, integrity, and availability of all MAHC information assets.

Scope

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

Policy Statement

At Muskoka Algonquin Healthcare (MAHC), personal health information (PHI) is protected to ensure patient privacy. Under the Personal Health Information Protection Act (PHIPA), and pursuant to Orders HO-004, HO-007 and HO-008 from the Office of the Information and Privacy Commissioner of Ontario, health care providers are prohibited from storing unencrypted PHI on portable devices or media.

Note: Storing large amounts of data on portable devices and media is of greater risk of loss, theft and inappropriate use or disclosure of considerable magnitude than storing or transporting PHI on paper.

Confidential corporate information (CCI) is protected to maintain the confidentiality, integrity, and availability of all MAHC information assets. Portable computing devices that MAHC information communication technology (ICT) provides will only be deployed once encryption software has been installed and confirmed operational in accordance with the Computer Workstations policy. Users are responsible for ensuring that user-owned portable devices and/or media are encrypted if used to store or transport PHI.

Non-compliance may result in disciplinary measures, up to and including termination.

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

Last Reviewed Date: 05/15/2018 00:00:00	Signing Authority: Senior Leadership Team
Next Review Date: 05/15/2021 00:00:00	Version: 2.0
Disclaimer Message: A printed copy of this document may not reflect the current, electronic version in the MAHC Document Management System (DMS). Any copies of this document appearing in paper form should always be checked against electronic version prior to use.	
Date/Time Generated: Nov 08, 2018 15:25	Generated By: gbin\tammy.tkachuk

	Policy/Procedure Name:	Portable Devices and Media
Manual: Administration	Number:	
Section: Risk Management	Effective Date:	01 Dec 2012
Pages: 2 of 4	Revision Date:	

- information that could expose the organization’s reputation to damage
- 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, Xrays, 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).

1. What is Personal Information (PI)?

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.

Last Reviewed Date: 05/15/2018 00:00:00	Signing Authority: Senior Leadership Team
Next Review Date: 05/15/2021 00:00:00	Version: 2.0
Disclaimer Message: A printed copy of this document may not reflect the current, electronic version in the MAHC Document Management System (DMS). Any copies of this document appearing in paper form should always be checked against electronic version prior to use.	
Date/Time Generated: Nov 08, 2018 15:25	Generated By: gbin\tammy.tkachuk

	Policy/Procedure Name:	Portable Devices and Media
Manual: Administration	Number:	
Section: Risk Management	Effective Date:	01 Dec 2012
Pages: 3 of 4	Revision Date:	

Portable devices – Mobile computing devices with information storage capabilities, including:

- mobile computer workstations (e.g., laptops, tablet PCs)
- personal digital assistants (including smart phones, e.g., BlackBerry, iPhone)

Portable media – Removable storage media, including:

- compact disks
- DVDs
- floppy disks
- USB keys
- external (backup) hard drives

Procedure

1. Protect PHI and CCI by carefully storing, transferring, transporting and disposing of portable devices and media containing PHI according to the following policies:
 - Storage, Transportation & Destruction of Confidential Information policy
 - Appropriate Use of Technology policy
 - Remote Access policy
 - MAHC Access, Use and Disclosure of Personal Health Information Policy
 - Records Retention & Destruction Policy
2. Store electronic files containing PHI or CCI on portable devices and/or media only if the requirements specified in the Storage, Transportation & Destruction of Confidential Information policy are met, including taking reasonable steps to safeguard devices when in use and in transit.
3. Comply with the Remote Access policy if using portable devices to access MAHC networks and applications remotely.
4. Report lost or stolen devices or media containing PHI or CCI to the Privacy Officer and complete an Incident Report.

Cross Reference

Storage, Transportation & Destruction of Confidential Information policy
 Appropriate Use of Technology policy
 Remote Access policy
 MAHC Access, Use and Disclosure of Personal Health Information Policy
 Records Retention & Destruction Policy

Notes

This material has been prepared solely for the use at Muskoka Algonquin Healthcare. Muskoka Algonquin Healthcare accepts no responsibility for the use of this material by any person or

Last Reviewed Date: 05/15/2018 00:00:00	Signing Authority: Senior Leadership Team
Next Review Date: 05/15/2021 00:00:00	Version: 2.0
Disclaimer Message: A printed copy of this document may not reflect the current, electronic version in the MAHC Document Management System (DMS). Any copies of this document appearing in paper form should always be checked against electronic version prior to use.	
Date/Time Generated: Nov 08, 2018 15:25	Generated By: gbin\tammy.tkachuk



	Policy/Procedure Name:	Portable Devices and Media
Manual: Administration	Number:	
Section: Risk Management	Effective Date: 01 Dec 2012	
Pages: 4 of 4	Revision Date:	

organization not associated with Muskoka Algonquin Healthcare. No part of this document may be reproduced in any form for publication without permission of Muskoka Algonquin Healthcare.

References / Relevant Legislation

Personal Health Information Protection Act, 2004

Last Reviewed Date: 05/15/2018 00:00:00	Signing Authority: Senior Leadership Team
Next Review Date: 05/15/2021 00:00:00	Version: 2.0
Disclaimer Message: A printed copy of this document may not reflect the current, electronic version in the MAHC Document Management System (DMS). Any copies of this document appearing in paper form should always be checked against electronic version prior to use.	
Date/Time Generated: Nov 08, 2018 15:25	Generated By: gbin\tammy.tkachuk