| MUSKOKA ALGONQUIN HEALTHCARE | | **Policy/Procedure Name:** | **Acceptable Use** |
|---|---|---|---|
| **Manual:** | Information & Communications Technology | **Number:** | |
| **Section:** | | **Effective Date:** | 01 Sept 2018 |
| **Pages:** | 1 of 9 | **Revision Date:** | DD MMM YYYY |

## Purpose

This acceptable use policy defines the information system security responsibilities and acceptable use rights for employees, volunteers, guests (including partners), vendors and contractors, students, medical students, residents, and medical professionals. This policy document includes an agreement form that, once signed, certifies the user's understanding and affirmation of the policy. These requirements are intended to help protect the confidentiality, integrity, and availability of data residing within Muskoka Algonquin Healthcare (MAHC) systems and specifically personal health information (PHI).

Muskoka Algonquin Healthcare provides computing devices, networks, and other electronic information systems to meet missions, goals and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets.

Resources include all platforms (e.g. operating systems, cloud solutions, etc.), all digital devices (e.g. computers, smart phones, tablets, mainframes, switches, routers, etc.), equipment (e.g. faxes, copiers, phones, etc.), network connections, applications (both developed in-house and acquired from third parties) and the data used, created by or contained within them.

Communications include but are not limited to: faxes, printed documents, recordings, phone calls, social media (e.g. Facebook, Google+, Twitter, Blogs YouTube, Instagram, etc.) and email.

## Scope

All employees, contractors, consultants, volunteers, temporary and other workers at MAHC, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by MAHC, or to devices that connect to a MAHC network or reside at a MAHC facility.

## Policy Statement

To protect the confidentiality, integrity and availability of MAHC's data by behaving in a manner consistent with MAHC's mission, vision and values and complying with all applicable laws, regulations, policies, standards and guidelines.

## Definitions

All information and data resources to which users are given access are to be used only to conduct the activities authorized by MAHC. The use of these resources must be conducted according to the policies, standards, and procedures instituted by MAHC or on its behalf. All individuals with access to MAHC data are responsible for the protection and confidentiality of such data. The unauthorized use or disclosure of information provided by these data processing systems may constitute a violation of MAHC, provincial, or federal laws which will result in disciplinary action consistent with the policies and procedures of MAHC – including employment termination.

Document Owner: The owner of this document is the Manager, Information Technology.

**Procedure**

# Policy Requirements

## Acceptable Usage

The resources provided by MAHC are to be utilized both responsibly and professionally; just because an action is technically possible does not mean that it is appropriate. Based on the following principles for acceptable use of MAHC resources, Users are:

- To protect the confidentiality, integrity and availability of MAHC data by behaving in a manner consistent with MAHC's mission, mission and values and complying with all applicable laws, regulations, policies, standards and guidelines**.**
- To comply with the policies, processes and guidelines for the specific resources to which they have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- To report any potential or identified privacy or security incident to the appropriate privacy or security staff.
- Allowed reasonable use (i.e. incidental personal use) of resources if:
    - Such use does not result in direct costs to MAHC;
    - Such use does not impact the reputation and community standing of MAHC;
    - There is no negative impact on users' performance of their duties and the use is prohibited.
- To respect the security and integrity of MAHC resources.

- To be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to utilize resources and show restraint in the consumption of shared resources.
- To respect the rights and property of others, including but not limited to; privacy, confidentiality and intellectual property (e.g. copyright, trademarks, etc.).
- Bound by the department's respective contractual and license agreements when using third party resources.
- To cooperate appropriately during incident response and investigation of potential unauthorized or illegal use of resources.
- All users should lock their computing devices when leaving their device unattended.

## Users may not:

- Attempt to disguise their identity, the identity of their account or the resource that they are using. Users may not attempt to impersonate another person (i.e. use another individual's account) or organization. Likewise, users shall not misuse or misrepresent MAHC's name, resource names, or network address spaces.
- Attempt to intercept, monitor (i.e. read), forge, alter (i.e. change) or destroy (i.e. delete) another User's communications.
- Use resources in a way that disrupts or adversely impacts (degrades performance of) their legitimate uses or creates interference with/for other users. Such conduct includes, but is not limited to: hacking; illegal peer-to-peer file sharing; unauthorized alteration of resources that are likely to result in the loss of work, resource downtime; or excessive consumption resulting in congestion that interferes with the work of others.
- Use resources in an unlawful or illegal manner, including but not limited to; cyberstalking; threats of violence; obscenity pornography; or any form that would constitute a criminal offence, a civil liability, or violation of any applicable law. In addition, users may not intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene. This provision applies to any digital communication distributed or sent with or while using MAHC resources.
- Use resources for private business, commercial or political activities, fundraising, non-departmental advertising, or activity that is prohibited by the MAHC Division of Human Resources.

- Download, install or run security software or utilities that reveals weaknesses in resources (e.g. vulnerability scanning, port mapping, network mapping, etc.); monitors or intercept communications (e.g. packet sniffers, keystroke loggers, etc.); or allows for the attempt to bypass security controls (e.g. password crackers, etc.).
- Knowingly take any action which has the likelihood of introducing any virus, Trojan, malware (spyware, botnet, ransomware, etc.) or other harmful software onto MAHC resources; nor should action be taken to deliberately circumvent controls designed to prevent such threats.
- Engage in the unauthorized copying, distributing, altering or translating of copyrighted or MAHC-owned materials, software, music or other media without the express permission of the copyright holder or as otherwise permitted by law.
- Use resources in a manner that allows for the unauthorized gathering, dissemination or disclosure of confidential data (social insurance numbers, Personally Identifiable Information (PII), credit card numbers, medical records, etc.).
- Extend, modify or retransmit network resources beyond what has been configured accordingly by MAHC through the installation of software or hardware (e.g. switches, routers, wireless access points, etc.)
- Share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or other similar information or devices used for identification and authorization purposes.
- Download MAHC data to personally owned devices.
- Attempt to obtain additional resources beyond those allocated or required to perform job functions, or circumvent information security measures.
- Never take a picture of data displayed on any MAHC system.

## Password Management

**All persons should:**

Choose passwords used to access MAHC information systems that are easy to remember but difficult to guess, where possible, use pass phrases when creating passwords (e.g., if33Lg00d!

for the phrase I feel good!). Passwords must contain eight characters and include at least three of the following:

- One number
- One uppercase letter
- One lowercase letter, or
- One special character

**Passwords must not include:**

- All or part of user ID
- Easily obtainable personal information (e.g., pets name, children's names birthdays or hobbies)
- Three consecutive characters (e.g., AAA)

**In Practice**

Passwords must be changed from any provided default password at initial logon.

Passwords must not be reused amongst systems (e.g., email, personal banking)

Passwords must remain secret and not be disclosed or shared even with system administrators, help desk personnel or managers.

Passwords must not be changed in an easily recognized pattern such as versioning (i.e. changing "if33Lg00d!1" to "if33Lg00d!2").

Passwords and IDs used to access Cerner must not be stored in any automated single sign-on process (SSO) solution except MAHC approved SSO management systems.

Passwords used to access Cerner must be committed to memory, unless stored securely without ID or name of application it is used for.

If there is suspicion that a password has been compromised immediately change the password and notify information security point of contact (e.g., helpdesk or Privacy Officer). Please refer to "Reporting Information Security Related Events" below.

## Protecting PHI

**All persons must:**

Never discuss PHI with any person that does not have a need-to-know or is not authorized to know the information.

Never discuss PHI in public areas, including elevators, as it may be easily overheard by those who do not have a need-to-know.

Never access PHI in non-private setting (e.g. coffee shops, airports, etc.) where unauthorized individuals can potentially view the information.

Secure access to PHI in any form (e.g., locking paper, printed copies originating from MAHC information systems or portable storage media in a cabinet) when left unattended in an unsecured area, especially when the office or area is vacated.

Always log-off or lock unattended computers or workstations to prevent unauthorized individuals from accessing PHI.

Only store PHI on [the EHR Solution]-approved devices or storage networks, and only store the minimal amount of PHI necessary on any encrypted portable storage media.

Always ensure that paper documents containing PHI are shredded or placed in a secure shredding receptacle when they are no longer needed.

Always use encryption when there is a requirement to transmit PHI (e.g. file transfer, email, etc.)

When required to leave a device in a vehicle ensure securely locked either in trunk or out of view before getting to your destination. If you get to the destination before securing the device you should take it with you.

Follow internal procedures for the proper secure disposal of any information technology that may have PHI stored on it.

Use approved remote access solution to remotely access EHR.

Use proper procedures to disconnect from a remote access connection (i.e. if disconnect or logoff option is present, use them rather than simply closing the application).

## Reporting Information Security Incidents

**All persons must:**
Immediately report suspected or confirmed information security incidents to MAHC information systems information security incident initial point of contact (e.g., a help desk). Alternatively, agents may report the incident to their manager or supervisor, who in turn must report it to the information security incident initial point of contact.

Provide their full cooperation to MAHC information systems Program Office, their agents or Electronic Service Providers with any information security incident investigation.

Examples of information security incidents include, but are not limited to:

- Unauthorized disclosure of PHI;
- Theft or loss of information technology that contains PHI even if it is encrypted;
- Virus or malware infection on a device that has access to MAHC information systems;
- Attempts (either failed or successful) to gain unauthorized access to MAHC information systems;
- Compromised password, i.e., another individual knows your password.

## Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with MAHC.

### Cross Reference

N/A

### Notes



### References / Relevant Legislation

#### Legislative

- PHIPA, ss. 12, 13 and Part V.1
- Ontario Regulation 329/04, s. 6

#### International Standards

- ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems – Requirements.
- ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management

- ISO/IEC 27005: 2008 Information Technology – Security Techniques – Information Security Risk Management
- ISO 27799:2008(E), Health Informatics – Information security management in health using ISO/IEC 27002

### eHealth Ontario EHR Policy Documents

- Information Security Policy
- Acceptable Use of Information and Information Technology
- Access Control and Identity Management Policy for System Level Access
- Local Registration Authority Procedures
- Identity Federation Standard
- Business Continuity Policy
- Cryptography Policy

## Appendices

## Appendix A: User Certification of Notification and Agreement of "Acceptable Use" Policy

**USER CERTIFICATION OF NOTIFICATION AND AGREEMENT OF COMPUTER USE POLICY**

I certify that I am an employee, volunteer, guest, vendor or contractor, student, medical student, resident or medical professional working for or on behalf of Muskoka Algonquin Healthcare Information Network and that I have read this "Acceptable Use Policy" and understand my obligations as described herein.

I understand that these obligations are not specific to any individual division or office of Muskoka Algonquin Healthcare, but are applicable to all employees, volunteers, and contractors of Muskoka Algonquin Healthcare.

I understand that failure to observe and abide by these obligations may result in disciplinary action, which may include dismissal and/or contract termination.

I also understand that in some cases, failure to observe and abide by these obligations may result in criminal or other legal actions.

Furthermore, I have been informed that Muskoka Algonquin Healthcare will retain this signed agreement on file for future reference. A copy of this agreement shall be maintained in the personnel file and/or in the contract administration file.

_____

Print Name

_____ _____

Employee, Volunteer, Guest, Vendor or Contractor, Student, Medical Student, Resident, Medical Professional Signature Date

_____ _____

MAHC Supervisor/MAHC Human Resources Signature Date