MUSKOKA ALGONQUIN HEALTHCARE		**Policy/Procedure Name:**	**Management of Personal Health Information Privacy Complaint or Breach**
Manual:	Administration	**Number:**	
Section:	Risk Management	**Effective Date:**	01 DEC 2012
Pages:	1 of 21	**Revision Date:**	15 JUN 2021

Table of Contents

Last Reviewed Date: 06/15/2021 00:00:00	**Signing Authority:** Senior Leadership Team
Next Review Date: 06/15/2024 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: Jun 27, 2023 11:27	**Generated By:** MAHC\allyson.snelling

Scope

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

Policy Statement

At Muskoka Algonquin Healthcare, all employees, physicians, students and volunteers are responsible for the protection of privacy and confidentiality of all written and electronic personal information and personal health information (PHI) following hospital PHI security methods, ensuring prompt investigation and containment and promptly reporting any complaints or breaches of confidentiality and/or security. Awareness of any such incidents may come directly from the affected person(s) or from other parties.

Definitions

Personal Health Information?
"Personal Information" is defined as recorded information about an identifiable individual. An individual's personal information **includes** information regarding his or her race, gender, home address, medical history, education history, identifying numbers (e.g. SIN, employee number, student number, etc.), financial or employment information, personal opinions, completed assignments and exams, and grades, comments and evaluations provided by an instructor.

It is mandatory that complaints and/or breaches be reported and addressed in a timely and standardized manner consistent with PHIPA to protect the privacy of patient's personal health information (PHI) contained in written or electronic formats from loss, theft, misdirection or inadvertent disclosure in accordance with the *Personal Health Information Protection Act* (PHIPA) legislation.

Under Section 72(2)(3)
" if an offence is committed under PHIPA, every officer, employee, physician, student, volunteer and affiliate of the hospital who authorized the offence, or had the authority to prevent the offence from being committed and knowingly refrained from doing so, is a party to and guilty of the offence. The individual is liable, on conviction, to the penalty for the offence, whether or not the hospital has been prosecuted or convicted."

Background

What is a privacy breach?

A privacy breach is an incident involving the unauthorized collection, use or disclosure of personal information. Unauthorized disclosures of personal information are the most common sources of privacy breaches and can occur when personal information is lost, stolen or inadvertently disclosed through human error.

Circumstances that could lead to a privacy breach include:

- loss or theft of equipment containing personal information (e.g., memory sticks, disks, laptops)
- e-mails sent to a wrong address or person
- incorrect file attached to an e-mail
- disposal of equipment containing personal information without secure destruction
- insufficient controls in place to protect personal information in paper and electronic files
- information faxed to a wrong number
- use of laptops, disks, memory sticks or other equipment to store or transport personal information outside of the office without adequate security measures

Levels of Privacy Breaches

Level I: Carelessness

When PHI is **carelessly** accessed, reviewed or disclosed by the individual or to others **without a legitimate need to know** or have authorization.

Examples include, but are not limited to:

- Discussing patient information in public areas
- Leaving a copy of patient information in a public area (meeting room, photocopier)
- Leaving a computer unattended in an accessible area with PHI unsecured

Level II: Curiosity

When an employee, physician, student, volunteer intentionally accesses or discloses PHI for purposes other than the care of the patient or for any other authorized purposes. Examples include, but are not limited to:

- Accessing a patient record of PHI out of curiosity
- Looking up images, pictures, addresses of relatives or friends or high profile individuals
- Accessing a patient record of PHI with a flagged sensitive status

Level III: Personal Gain or Malice

When an employee, physician, student, volunteer accesses or discloses PHI for personal gain or with malicious intent. Examples include, but are not limited to:

- Accessing or disclosing PHI of relatives or friends or high profile individuals relating to the provision of their healthcare (i.e. reason for visit, diagnosis, legal status, etc.)
- Compiling a mailing list for personal use or to sell

Procedure

All MAHC employees, physicians, students and volunteers shall report directly to their manager immediately and complete an incident report via IMS if they become aware of:

- a public complaint regarding a breach of personal health information/personal information
- an incident regarding unauthorized collection, use or disclosure of personal health information/personal information
- any compromise of confidentiality and security of information, or security systems containing personal health information/personal information

Managers shall in turn promptly notify the Privacy Officer (or delegate). The Manager and Privacy Officer will promptly initiate an investigation of the complaint or breach and compile the facts as follows:

The Manager and/or Privacy Officer will:

1. Initiate steps to contain the complaint or breach including further containment to the collection, use or disclosure of PHI.
2. Consult with the Human Resources Manager.
3. Conduct an investigation, gathering facts related to the complaint or breach (appendix a).
4. The Manager and/or Privacy Officer will complete an Incident Report and include improvements recommended with respect to the related information handling practices/procedures or security processes.
5. Upon conclusion of the investigation and outcome, the completed incident report will be submitted to administration for inclusion in the incident reporting to Quality Council.
6. If appropriate, alert the Information Technology department to monitor case related collection, use or disclosure activities.

Post investigation of unauthorized collection, use and disclosure, the Manager and/or Privacy Officer will:

1. Examine the related information handling practices and procedures or security processes;
2. The Privacy Officer will notify the Chief Executive Officer in writing through a briefing note regarding the outcome of each complaint or breach, summarizing additional recommendations for the prevention of any future similar incidents;
3. The Privacy Officer will collaborate to implement approved steps to address/prevent future occurrences;
4. The Privacy Officer will take prompt steps to notify and apologize to affected persons including responding in writing

Reporting a Privacy Breach to the Commissioner

To strengthen the privacy protection of personal health information, the Ontario government has amended the Personal Health Information Protection Act (the act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches, effective October 1, 2017.

As a custodian, we must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, we must report it.

It is important to remember that even if you do not need to notify the Commissioner, we have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

Annual Statistic Reporting to IPC

Starting in March 2019 health information custodians will be required to provide our office with an annual report on the number of privacy breaches that occurred during the previous calendar year.

Under the Personal Health Information Protection Act, custodians must inform IPC of incidents where personal health information in their care was lost, stolen, or used or disclosed without authorization. (see appendices)

1.1 Use or disclosure without authority

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian.

Example: when a person looks at an ex-spouse's medical history for no work related purpose ("snooping").

Example: where hospital employees are curious about why a local celebrity or co-worker was treated at the hospital and access that individual's medical records. This includes situations where the unauthorized use or disclosure is not done for a personal or malicious motive.

We generally do not need to notify the Commissioner when the breach is accidental, for example, when information is inadvertently sent by email or faxed to the wrong person, or a letter is placed in the wrong envelope.

Also, we do not need to notify the Commissioner when a person who is permitted to access patient information accidentally accesses the wrong patient record.

1.2 Stolen information

A typical example of this would be where someone has stolen paper records, or a laptop or other electronic device. Another example would be where patient information is subject to a ransomware or other malware attack, or where the information has been seized through use of a portable storage device.

We do not need to notify the Commissioner if the stolen information was de-identified or properly encrypted.

Example: where someone has stolen paper records, or a laptop or other electronic device.

Example: where patient information is subject to a ransomware or other malware attack, or where the information has been seized through use of a portable storage device.

Not required to report when the stolen information was de-identified or properly encrypted.

1.3 Further use or disclosure without authority after a breach

Following an initial privacy breach, you may become aware that the information was or will be further used or disclosed without authority; we must report this to the Commissioner.

Example: where employee inadvertently sends a fax containing PHI to the wrong person. Although the person returned the fax to you, you learn that he kept a copy and is threatening to make the information public.

Example: Where you learn that an employee wrongfully accessed patient information and subsequently used this information to market products or services or to commit fraud.

1.4 Pattern of similar breaches

Even if a privacy breach is accidental or insignificant by itself, it must be reported to the Commissioner if it is part of a pattern of similar breaches. Such a pattern may reflect systemic issues that need to be addressed, such as inadequate training or procedures.

We must use our judgment in deciding if a privacy breach is an isolated incident or part of a pattern; take into account, for instance, the time between the breaches and their similarities. Keeping track of privacy breaches in a standard format will help you identify patterns.

Example: you discover that a letter to a patient inadvertently included information relating to a different patient. Over a few months, the same mistake is repeated several times because an automated process for generating letters has been malfunctioning for some time.

1.5 Disciplinary action against a college member

A duty to report an employee or other agent to a health regulatory college also triggers a duty to notify the Commissioner.

Where an *employee* is a member of a college, you must notify the Commissioner of a privacy breach if you discipline them as a result of the breach or they resign and you believe this action is related to the breach.

Where a *health care practitioner with privileges or otherwise affiliated with you* is a member of a college, you must notify the Commissioner of privacy breach if:

- we revoke, suspend or restrict their privileges or affiliation as a result of the breach
- they relinquish or voluntarily restrict their privileges or affiliation and we believe this action is related to the breach

Similar requirements apply to *health care practitioners employed by a board of health*

1.6 Disciplinary action against a non-college member

Not all employees or other agents of a custodian are members of a college. If an agent is not such a member, the same notification rules apply to circumstances that would have triggered notification to a college, had the agent been a member.

> Example: where one of your registration clerks has an unpleasant encounter with a patient and posts information about the patient on social media. The hospital disciplines the clerk. Although the clerk is not a member of a college, you must report this privacy breach.

1.7 Significant breach

Even if none of the above six circumstances apply, you must notify the Commissioner if the privacy breach is significant. In deciding whether a breach is significant, you must consider all the relevant circumstances, including whether

i. the information is sensitive
ii. the breach involves a large volume of information
iii. the breach involves many individuals' information
iv. more than one custodian or agent was responsible for the breach

Even breaches that cause no particular harm may still be significant.

> Example: Disclosure of a patient's mental health assessment on a group distribution list, rather than just the patient's physician.
>
> Example: You post detailed information on a website about a group of patients receiving specialized treatment for a novel health issue. While you didn't use any patients' names, other can easily identify them.

Note: Consider consulting with legal in these circumstances.

Annual Report to the Commissioner

Custodians will be required to start tracking privacy breach statistics as of January 1, 2018 and will be required to provide the Commissioner with an annual report of the previous calendar year's statistics, starting in March 2019.

The Commissioner will release detailed guidance on this statistical reporting requirement in fall 2017.

Notes

References / Relevant Legislation

Personal Health Information Protection Act

Appendices

Appendix 1 - Annual Reporting of Privacy Breach Statistics to the Commissioner, November 2017
Appendix 2 - Reporting a Privacy Breach to the Commissioner, September 2017
Appendix 3 – Documentation and Consultation Record

Appendix 1 - Annual Reporting of Privacy Breach Statistics to the Commissioner

NOVEMBER 2017

Annual Reporting of Privacy Breach Statistics to the Commissioner

REQUIREMENTS FOR THE HEALTH SECTOR

Starting in March 2019 health information custodians will be required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

(1) On or before March 1, in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.
3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's custody or control was disclosed without authority.

(2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

For custodians to prepare for this reporting requirement, they must start tracking their privacy breach statistics as of January 1, 2018. The following is the information the IPC will require in the annual report.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Custodians should maintain this information to ensure they are ready to report on the 2018 calendar year in early 2019:

STOLEN PERSONAL HEALTH INFORMATION

- Total number of incidents where personal health information was stolen
- Of the total in this category, the number of incidents where:
  - theft was by an internal party (such as an employee, affiliated health practitioner or electronic service provider)
  - theft was by a stranger
  - theft was the result of a ransomware attack
  - theft was the result of another type of cyberattack
  - unencrypted portable electronic equipment (such as USB keys or laptops) was stolen
  - paper records were stolen
- Of the total in this category, the number of incidents where:
  - one individual was affected
  - 2 to 10 individuals were affected
  - 11 to 50 individuals were affected
  - 51 to 100 individuals were affected
  - over 100 individuals were affected

LOST PERSONAL HEALTH INFORMATION

- Total number of incidents where personal health information was lost
- Of the total in this category, the number of incidents where:
  - loss was a result of a ransomware attack
  - loss was the result of another type of cyberattack
  - unencrypted portable electronic equipment (such as USB keys or laptops) was lost
  - paper records were lost
- Of the total in this category, the number of incidents where:
  - one individual was affected
  - 2 to 10 individuals were affected
  - 11 to 50 individuals were affected

- 51 to 100 individuals were affected
- over 100 individuals were affected

USED WITHOUT AUTHORITY

- Total number of incidents where personal health information was used (e.g. viewed, handled) without authority
- Of the total in this category, the number of incidents where:
  - unauthorized use was through electronic systems
  - unauthorized use was through paper records
- Of the total in this category, the number of incidents where:
  - one individual was affected
  - 2 to 10 individuals were affected
  - 11 to 50 individuals were affected
  - 51 to 100 individuals were affected
  - over 100 individuals were affected

DISCLOSED WITHOUT AUTHORITY

- Total number of incidents where personal health information was disclosed without authority
- Of the total in this category, the number of incidents where:
  - unauthorized disclosure was through misdirected faxes
  - unauthorized disclosure was through misdirected emails
- Of the total in this category, the number of incidents where:
  - one individual was affected
  - 2 to 10 individuals were affected
  - 11 to 50 individuals were affected
  - 51 to 100 individuals were affected
  - over 100 individuals were affected

NOTES:

Do not count each incident more than once. If one incident includes more than one of the above categories, choose the category that it best fits. For example, if an employee accessed personal health information without authority, and then disclosed the information, count that incident as either a use or a disclosure, but not both.

In this annual statistics report, you must include all thefts, losses, or unauthorized uses or disclosures, even if you were not required to report them to the IPC under Section 6.3 of the Regulation.

Health privacy breach statistics will be collected through the IPC's Online Statistics Submission Website in early 2019. Custodians will find it easier to provide the IPC with the information required at that time if they keep track of these statistics over the course of 2018.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Appendix 2 - Reporting a Privacy Breach to the Commissioner

SEPTEMBER 2017

Reporting a Privacy Breach to the Commissioner

GUIDELINES FOR THE HEALTH SECTOR

To strengthen the privacy protection of personal health information, the Ontario government has amended the *Personal Health Information Protection Act* (the act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. This law takes effect **October 1, 2017**.

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it. The following is a summary—for the complete wording of the regulation, see the appendix at the end of this document.

It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

1. Use or disclosure without authority

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

person looks at an ex-spouse's medical history for no work related purpose—the "snooping" case. That person could be your employee, a health care practitioner with privileges, a third party (such as a service provider), or even someone with no relationship to you.

This includes situations where the unauthorized use or disclosure is not done for a personal or malicious motive. For example, it might include where employees of a hospital are curious about why a local celebrity or a co-worker was treated at the hospital, and access that individual's medical records.

You generally do not need to notify the Commissioner when the breach is accidental, for example, when information is inadvertently sent by email or courier to the wrong person, or a letter is placed in the wrong envelope. Also, you do not need to notify the Commissioner when a person who is permitted to access patient information accidentally accesses the wrong patient record. However, even accidental privacy breaches must be reported if they fall into one of the other categories below.

2. Stolen information

A typical example of this would be where someone has stolen paper records, or a laptop or other electronic device. Another example would be where patient information is subject to a ransomware or other malware attack, or where the information has been seized through use of a portable storage device. You should report cases like these to the Commissioner.

You do not need to notify the Commissioner if the stolen information was de-identified or properly encrypted.

3. Further use or disclosure without authority after a breach

Following an initial privacy breach, you may become aware that the information was or will be further used or disclosed without authority; you must report this to the Commissioner.

For example, your employee inadvertently sends a fax containing patient information to the wrong person. Although the person returned the fax to you, you learn that he kept a copy and is threatening to make the information public. Even if you did not report the initial incident, you must notify the Commissioner of this situation.

Other examples include where you learn that an employee wrongfully accessed patient information and subsequently used this information to market products or services or to commit fraud (e.g., health care or insurance fraud).

4. Pattern of similar breaches

Even if a privacy breach is accidental or insignificant by itself, it must be reported to the Commissioner if it is part of a pattern of similar breaches. Such a pattern may reflect systemic issues that need to be addressed, such as inadequate training or procedures.

You must use your judgment in deciding if a privacy breach is an isolated incident or part of a pattern; take into account, for instance, the time between the breaches and their similarities. Keeping track of privacy breaches in a standard format will help you identify patterns.

For example, you discover that a letter to a patient inadvertently included information relating to a different patient. Over a few months, the same mistake is repeated several times because an automated process for generating letters has been malfunctioning for some time. This should be reported to the Commissioner.

5. Disciplinary action against a college member

A duty to report an employee or other agent to a health regulatory college also triggers a duty to notify the Commissioner.

Where an *employee* is a member of a college, you must notify the Commissioner of a privacy breach if:

- you terminate, suspend or discipline them as a result of the breach
- they resign and you believe this action is related to the breach

Where a *health care practitioner with privileges or otherwise affiliated with you* is a member of a college, you must notify the Commissioner of a privacy breach if:

- you revoke, suspend or restrict their privileges or affiliation as a result of the breach
- they relinquish or voluntarily restrict their privileges or affiliation and you believe this action is related to the breach

Similar requirements apply to *health care practitioners employed by a board of health*.

6. Disciplinary action against a non-college member

Not all employees or other agents of a custodian are members of a college. If an agent is not such a member, you must still notify the Commissioner in the same circumstances that would have triggered notification to a college, had the agent been a member.

For example, one of your registration clerks has an unpleasant encounter with a patient and posts information about the patient on social media. You suspend the clerk for a month. Although the clerk is not a member of a college, you must report this privacy breach.

7. Significant breach

Even if none of the above six circumstances apply, you must notify the Commissioner if the privacy breach is significant. In deciding whether a breach is significant, you must consider all the relevant circumstances, including whether

i. the information is sensitive
ii. the breach involves a large volume of information
iii. the breach involves many individuals' information
iv. more than one custodian or agent was responsible for the breach

For example, you are a health care practitioner who accidentally discloses a patient's mental health assessment to other practitioners on a group email distribution list, rather than to just the patient's physician. This information is highly sensitive and has been disclosed to a number of persons to whom you did not intend to send the information. Or, you post detailed information on a website about a group of patients receiving specialized treatment for a novel health issue. It comes to your attention that while you did not use any patients' names, others can easily identify them. This breach involves many patients, whose information has potentially been made widely available. These types of breaches should be reported to the Commissioner. Note that even breaches that cause no particular harm may still be significant.

ANNUAL REPORT TO THE COMMISSIONER

Custodians will be required to start tracking privacy breach statistics as of January 1, 2018, and will be required to provide the Commissioner with an annual report of the previous calendar year's statistics, starting in March 2019.

The Commissioner will release detailed guidance on this statistical reporting requirement in fall 2017.

APPENDIX

Ontario Regulation 329/04 under the *Personal Health Information Protection Act*, section 6.3:

(1) The following are the circumstances in which a health information custodian is required to notify the Commissioner for the purposes of section 12(3) of the Act:

1. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing the information without authority.
2. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was stolen.
3. The health information custodian has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in the custodian's custody or control, the personal health information was or will be further used or disclosed without authority.
4. The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information in the custody or control of the health information custodian.
5. The health information custodian is required to give notice to a College of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.
6. The health information custodian would be required to give notice to a College, if an agent of the health information custodian were a member of the College, of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.
7. The health information custodian determines that the loss or unauthorized use or disclosure of personal health information is significant after considering all relevant circumstances, including the following:
   i. Whether the personal health information that was lost or used or disclosed without authority is sensitive.
   ii. Whether the loss or unauthorized use or disclosure involved a large volume of personal health information.

iii. Whether the loss or unauthorized use or disclosure involved many individuals' personal health information.

iv. Whether more than one health information custodian or agent was responsible for the loss or unauthorized use or disclosure of the personal health information.

(2) In this section,

"College" means a College as defined in subsection 17.1 (1) of the Act.

Appendix 3 – Document Consultation & Approval Tracking Record

Document Title: _____

Document Status:
- ☐ New
- ☒ Revision of Existing
- ☐ Reviewed, no edits required

Document Type:
- ☒ Policy/Procedure
- ☐ Protocol/Guideline
- ☐ Standard Operating Procedure
- ☐ Medical Directive
- ☐ Order Set
- ☐ Other: _____
- ☐ Clinical Pathway
- ☐ Order Set
- ☐ Standard of Care
- ☐ Rules & Regulations
- ☐ Form

Development Team (list the names and designations of those involved in the development/review of the document)**:**

Name	Designation
Frankie Dewsbury	**Director, Projects, Quality, Risk & PFAC**

Scope of Document:
☐ Department specific ☐ Two or more departments/services ☒ Corporate/Hospital-wide

Groups Impacted by Document:
- ☐ Nursing
- ☐ Credentialed Staff
- ☐ Clerical/Support Staff
- ☐ Administration
- ☐ All Staff/Credentialed Staff
- ☐ Allied Health (specify):
- ☐ Support Staff (specify):
- ☐ Other (specify):

Consultation Phase (list below the stakeholders/committees that will provide feedback and input into the document prior to submission to the Signing Authority for final approval):

Stakeholder/Committee	Date Consulted	Feedback/Comments	Development Team Response

Education & Communication Plan: (select all that apply)

Tool(s) / Method(s)	*Timeline for Completion*	*Lead Responsible*
☐ Huddles/Staff meetings		
☐ Education Blitzes		
☐ Learning Management System (LMS) Module		
☐ Posters		
☐ Electronic Mail		
☐ Communication Binder		
☐ Department Meetings		
☐ Frequently Asked Questions (FAQ)		

MUSKOKA ALGONQUIN HEALTHCARE	**Policy/Procedure Name:**	**Management of Personal Health Information Privacy Complaint or Breach**
Manual: Administration	**Number:**	
Section: Risk Management	**Effective Date:**	01 DEC 2012
Pages: 21 of 21	**Revision Date:**	15 JUN 2021

☐ Memo		
☐ MAHC Matters		
☐ Other:		

Approval Phase (for list of Signing Authorities, view the "Policy, Procedure and Guideline Development" policy)**:**

Signing Authority: **Senior Leadership Team** | **Date Review:** **June 15 2021** | ☒ **Approved** | ☐ **Not Approved**

Comments: No material revisions

DOCUMENT MANAGEMENT SYTEM INFORMATION (complete for the purpose of uploading to the DMS via executive assistant/document support person assigned to portfolio)
1. Category(manual/section):
2. Key Words: *(Indicate if there are any additional key words or common words used by staff to reference the document that should be added beyond what is currently in the purpose or policy statements.)*
3. Is this document an ROP (Required Organizational Practice):
4. Is there a preferred URL or external link:
5. Who will be accountable for leading any policy review?
6. Review Period: *(Indicate is the review period is less than three year. All documents must be reviewed at least every three years.)*

Last Reviewed Date: 06/15/2021 00:00:00	**Signing Authority:** Senior Leadership Team
Next Review Date: 06/15/2024 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: Jun 27, 2023 11:27	**Generated By:** MAHC\allyson.snelling