| McLaren HEALTH CARE | | Policy Title: | HIPAA Privacy and Security Breaches, Notifications, and Mitigation |
|---|---|---|---|
| **Effective Date:** | January 18, 2011 | **Policy Number:** | MHC_CC1109 |
| **Review Date:** | | **Section:** | Compliance |
| **Revised Date:** | January 11, 2022 | **Oversight Level:** | Corporate |
| **Administrative Responsibility:** | Corporate VP of Compliance; HIPAA Council | | |

## 1. Purpose

**1.1.** This document sets forth the policy and procedures to comply with the HIPAA Rules Regarding Breaches of Protected Health Information.

## 2. Scope

**2.1.** McLaren Health Care Corporation ("MHC"), its subsidiaries, any other entity or organization in which MHC or an MHC subsidiary owns a direct or indirect equity interest of 50% or more, provided that organization has agreed to adopt MHC policies; and MHC's workforce members, including employees and contracted agents, physicians, volunteers, vendors/suppliers, and other business partners.

**2.2.** Business Associates of MHC and its subsidiaries, including organized health care arrangements in which they participate, as required by the HIPAA Rules.

## 3. Definitions

**3.1. Breach** means the acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI.

**3.1.1.** Breach excludes:

**3.1.1.1.** Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA Rules.

**3.1.1.2.** Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or Business Associate to another person authorized to access PHI at the same covered entity or Business Associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the Privacy Rule.

**3.1.1.3.** A disclosure of PHI where a covered entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

**3.1.2.** Except as provided in 3.1.1, an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a Breach unless

MHC or its Business Associate, as applicable, demonstrates that there is a low probability that the Protected Health Information has been compromised based on a Risk Assessment.

**3.2. Business Associate** means an organization or a person, other than a Workforce Member who:

**3.2.1.** On behalf of MHC, creates, receives, maintains, or transmits PHI for:

**3.2.1.1.** claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; patient safety activities; billing; benefit management; practice management; and repricing; or

**3.2.2.** Provides one of the following services which involves the disclosure of PHI from MHC or another Business Associate:

**3.2.2.1.** legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; or financial services to MHC;

**3.2.3.** Provides data transmission services which routinely require access to PHI;

**3.2.4.** Provides personal health records to one or more Individuals on behalf of MHC;

**3.2.5.** Is a Subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate;

**3.2.6.** Business Associate does not include:

**3.2.6.1.** Subsidiaries or other covered entities which are part of an MHC organized health care arrangement;

**3.2.6.2.** Government agencies that determine eligibility for a government health plan;

**3.2.6.3.** A plan sponsor making disclosures for its group health plan.

**3.3. Discovery or "Discovered"** is defined as the first day on which a Breach is known or, by exercising reasonable diligence, would have been known. MHC shall be deemed to have knowledge of a Breach if it is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of MHC.

**3.4. HIPAA Rules** means the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and implementing regulations, the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") the Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule"), Standards for Electronic Transactions, and the privacy, security and Breach Notification regulations of the Health Information Technology for Economic and Clinical Health Act ("HITECH Rules") and HIPAA Omnibus final rule.

**3.5. Individual** means the person who is the subject of PHI or the Authorized Representative acting on behalf of the Individual.

**3.6. Next of Kin** includes the following persons in order of priority:

3.6.1. Spouse

3.6.2. Adult Children

3.6.3. Mother or Father

3.6.4. Adult Siblings

3.6.5. Other persons authorized or obligated to provide care.

3.7. **Organized Health Care Arrangement (OHCA)** is an organized system of health care where the various components of the Corporation hold themselves out to the public as participating in a joint arrangement, and jointly perform treatment, payment, and/or operations including utilization review and quality assessment and improvement activities; and one or more group health plans maintained by the same plan sponsor; and the Board of Directors of the Corporation has determined that the creation of an "Organized Health Care Arrangement," as defined in 45 C.F.R. §164.501, would permit the components of the Corporation to perform services for their patients and plan participants more efficiently and effectively.

3.8. **Personal Representative** (Authorized Representative) is defined as the person who has the authority, granted by the Probate Court, to act on behalf of a Deceased Individual or the Individual's estate.

3.9. **Protected Health Information (PHI) and/or Patient Record** is defined as any Individually identifiable health information that is collected from an Individual, and is transmitted, received, created and/or maintained, in any form or medium, by MHC and/or its subsidiaries.

3.9.1. PHI is any information that:

3.9.1.1. Relates to the past, present or future physical or mental health/condition of an Individual.

3.9.1.2. Relates to the provision of health care to an Individual.

3.9.1.3. Relates to the past, present, or future payment for the provision of health care to an Individual.

3.9.2. PHI is any information that either identifies the Individual or there is a reasonable basis to believe the information can be used to identify the Individual. Examples include, but are not limited to:

3.9.2.1. name, medical record number, encounter number, social security number, address, and photo, diagnosis, diagnostic reports, procedures, progress notes, images, medications, billing documents, physician or location (if such information leads one to know or infer a diagnosis, etc.), slides, and/or blocks.

3.9.3. PHI excludes:

3.9.3.1. Records of students maintained by federally funded educational agencies: covered by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g; or maintained by a healthcare provider and used only for the treatment of students 18 years or older, or attending post-secondary educational institutions, 20 U.S.C. 1232g(a)(4)(B)(iv);

3.9.3.2. Employment records held by MHC in its role as employer; and

3.9.3.3. Records of a person who has been deceased more than 50 years.

3.10. **Risk Assessment** means a review of at least the following factors:

3.10.1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

3.10.2. The unauthorized person who used the PHI or to whom the disclosure was made;

3.10.3. Whether the PHI was actually acquired or viewed; and

3.10.4. The extent to which the risk to the PHI has been mitigated.

3.11. **Secretary** means the Secretary of Health and Human Services.

3.12. **Subcontractor** is a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.

3.13. **Unsecured PHI** is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized person(s) through the use of a technology or methodology specified by the Secretary in guidance if one or more of the following applies:

3.13.1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been Breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

3.13.1.1. Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

3.13.1.2. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52 and amendments, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

3.13.2. The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

3.13.2.1. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

3.13.2.2. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

3.14. Workforce / Workforce Members is defined as employees, temporary workers, contracted agents, physicians, volunteers, vendors/suppliers, consultants, students and other persons or entities whose conduct in the performance of work is under the direct control of MHC or its Business Associate, whether or not they are paid by MHC or its Business Associate.

## 4. Policy

4.1. Breach Notification Requirements. The Compliance Officer or Corporate Vice President of Compliance must be notified of any actual or potential Breach of Unsecured PHI, immediately upon Discovery.

4.2. Risk Assessment. MHC will conduct a Risk Assessment for each actual or potential Breach and document findings in the Breach Risk Assessment Tool (Appendix 7.3).

4.2.1. MHC has the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of Unsecured PHI did not constitute a Breach.

4.3. Notification. Unless the Compliance Officer, or designee, determines, based on the Risk Assessment, that there is a "low probability" that the PHI has been compromised, MHC must provide notification of the Breach to affected Individuals, the Secretary, and, in certain circumstances, the media. In addition, Business Associates must notify MHC that a Breach has occurred.

4.3.1. *Notice to Individuals*. MHC must notify affected Individuals following the Discovery of a Breach of Unsecured PHI.

4.3.1.1. MHC must provide the Individuals notice in written form by first-class mail, or alternatively, by Email if the affected Individual has agreed to receive such notices electronically. The notice must be written in plain language.

4.3.1.2. If the Individual is deceased and MHC has the address of the Next of Kin or Personal Representative, written notice by first-class mail to the Next of Kin or Personal Representative of the Individual. Substitute notice is not required in the case in which there is insufficient or out-of-date contact information that precludes written notification to the Next of Kin or Personal Representative of an Individual.

4.3.1.3. If MHC has insufficient or out-of-date contact information for 10 or more Individuals, including deceased Individuals, MHC must provide substitute notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected Individuals likely reside. The substitute notice shall:

4.3.1.3.1. Be in the form of either a conspicuous posting for a period of 90 days on the home page of the website of the MHC entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the Individuals affected by the Breach likely preside; and

4.3.1.3.2. Include a toll-free phone number that remains active for at least 90 days where an Individual can learn whether the Individual's Unsecured PHI may be included in the Breach.

4.3.1.4. If MHC has insufficient or out-of-date contact information for fewer than 10 Individuals, MHC may provide substitute notice by an alternative form of written notice, telephone, or other means.

4.3.1.5. Additional Notice in Urgent Situations. In any case deemed by MHC to require urgency because of possible imminent misuse of Unsecured PHI, the information may be provided to the Individuals by telephone or other means, as appropriate, in addition to the required written notice.

4.3.1.6. Timing and Content of Notice. Individual notifications must be provided without unreasonable delay and in no case later than 60 calendar days following the Discovery of a Breach and must include, to the extent possible:

4.3.1.6.1. a brief description of the Breach, including the date of the Breach, and the date of the Discovery of the Breach;

4.3.1.6.2. a description of the types of Unsecured PHI that was involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information involved);

4.3.1.6.3. the steps affected Individuals should take to protect themselves from potential harm;

4.3.1.6.4. a brief description of what the covered entity is doing to investigate the Breach, to mitigate harm to Individuals, and prevent further Breaches; and

4.3.1.6.5. Contact information of the entity Privacy Officer; including a toll-free number, an Email address, Website, or postal address for Individuals to ask questions or learn additional information.

4.3.2. *Notice to the Media*. If MHC experiences a Breach affecting more than 500 residents of a State or jurisdiction, in addition to notifying the affected Individuals, MHC is required to provide notice to prominent media outlets serving the State or jurisdiction.

4.3.2.1. MHC will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like Individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 calendar days following the Discovery of a Breach and must include the same information required for the Individual notice.

4.3.3. *Notice to the Secretary*. MHC will notify the Secretary by visiting the HHS Website and filling out and electronically submitting a Breach report form.

4.3.3.1. If a Breach affects 500 or more Individuals, MHC must notify the Secretary without unreasonable delay and in no case later than 60 calendar days following the Breach.

**4.3.3.2.** If a Breach affects fewer than 500 Individuals, MHC may notify the Secretary of such Breaches without unreasonable delay following the conclusion of the investigation, but no later than 60 days after the end of the calendar year in which the Breach was discovered.

**4.4. Notification of a Breach by a Business Associate or a Business Associate's Subcontractor.** If a Breach of Unsecured PHI occurs at or by a Business Associate, or a Subcontractor of the Business Associate, the Business Associate must notify MHC immediately following the Discovery of the Breach and at a minimum within five (5) business days, unless otherwise specified in the Business Associate Agreement. See MHC_CC1106 Business Associate and Data Use Agreements for detail.

**4.4.1.** *Breach Information*. The Business Associate must provide MHC with:

**4.4.1.1.** the identification of each Individual affected by the Breach as well as:

**4.4.1.2.** a complete description of the Breach, including the date of the Breach, and the date of the Discovery of the Breach; and

**4.4.1.3.** a description of the types of Unsecured PHI that was involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information involved) .

**4.4.2.** *Notification*. At MHC's option, or as specified in the Business Associate Agreement, the Business Associate will notify Individuals under the direction of MHC Privacy Officer or designee, or cover the associated costs incurred by MHC if MHC provides notice to Individuals.

**4.4.3.** *Mitigation*. In accordance with the Business Associate Agreement the Business Associate will be responsible to mitigate to the extent practicable the Breach to the Individual(s).

**4.4.4.** *Remediation*. The Business Associate will provide MHC with an analysis of causes, a plan of correction and provide periodic reports on remediation progress.

**4.5. Law Enforcement Delay.** If a law enforcement official states to MHC or Business Associate that a notification, notice, or posting required by this Policy would impede a criminal investigation or cause damage to national security, MHC or its Business Associate shall:

**4.5.1.** If the statement is in writing and specifies the time for which the delay is required, delay such notification, notice, or posting for the time period specified by the official; or

**4.5.2.** If the statement is made orally, document the statement, including the identity of the official making the statement, and delay notification, notice or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

**4.6. Institutional Actions.** At least annually, the Corporate HIPAA Council will review all incidents of actual or potential Breaches and make recommendations to the MHC Corporate Compliance Committee regarding institutional improvements required to minimize such occurrences in the future and to identify any changes in risk.

## 5. Procedure

**5.1. Breach Notice Procedures.** Once the Risk Assessment process is complete and it is determined by the Compliance or Privacy Officer that a Breach of Unsecured PHI has occurred, MHC must provide notification to the Individuals, to the Secretary, and as defined by the Policy to the media.

**5.1.1.** The Compliance or Privacy Officer will also immediately report the breach to the MHC Vice President of Compliance, who will notify the Risk and Insurance Department if the breach involves a data breach or cybersecurity concern so the cyber liability carrier can be notified when appropriate.

**5.2. Notification.** The Compliance or Privacy Officer will determine whether the breach requires reporting to the Individual, Secretary, and/or media based on the Risk Assessment process.

**5.2.1.** *Notice to the Individuals*. The Privacy Officer will provide Notice to Individuals without unreasonable delay and in no case later than 60 calendar days from the first day on which such Breach is Discovered.

**5.2.1.1.** The notice will be provided as required by this policy.

**5.2.1.2.** The notice will be written in plain language and must contain the information as described in Section 4.3.

**5.2.2.** *Credit Monitoring Provisions*:

**5.2.2.1.** The Privacy Officer will determine the need for up to one year of credit monitoring based on the outcome of the Risk Assessment. Refer to MHC_CC1109.7.4.)

**5.2.2.2.** The administrative approval process is required for greater than one year of credit monitoring.

**5.2.3.** *Media Notice*. If MHC experiences a Breach affecting more than 500 Individuals, the Privacy Officer, under the guidance of the Marketing and Communications Department, will provide notice to prominent media outlets serving the State or jurisdiction. The Notice will be provided in the form of a press release. Media notification must be provided without unreasonable delay and in no case later than 60 calendar days following the discovery of a Breach and must include the same information required for the Individual notice.

**5.2.4.** *Notice to the Secretary*. This notice must be submitted electronically by the Privacy Officer completing all information required on the online Breach notification form available at https://ocrportal.hhs.gov/ocr/breach (see appendix).

**5.2.4.1.** For Breaches that affect fewer than 500 Individuals, the Privacy Officer must provide the Secretary with notice. All notifications of Breaches must be submitted at the conclusion of the investigation, but no later than 60 days from the end of the calendar year in which the Breach occurred. This notice must be submitted electronically by following the link above and completing all information required on the Breach notification form. A separate form must be completed for every Breach that has occurred during the calendar year.

5.2.4.2. If a Breach affects 500 or more Individuals, the Privacy Officer must provide the Secretary with notice of the Breach without unreasonable delay and in no case later than 60 calendar days from discovery of the Breach. This notice must be submitted electronically by following the link above and completing all information required on the Breach notification form.

5.2.4.3. If the Privacy Officer has submitted a Breach notification form to the Secretary and discovers additional information to report, he/she must submit an additional form, checking the appropriate box to signal that it is an updated submission.

5.3. Notification of a Breach by a Business Associate. The MHC Privacy Officer will obtain from the Business Associate the information as described in Section 4.4. The Business Associate may complete the Breach Notification Risk Assessment Tool (MHC_CC1109.7.3b) to provide the necessary information to MHC.

5.3.1. The MHC Privacy Officer will direct and oversee provision of notice to the Individuals if provided by the Business Associate, or provide the notice to the Individuals.

5.3.1.1. If providing notice, the Business Associate has the burden of proof to demonstrate that all required notifications have been provided.

5.3.2. The Privacy Officer will work with the Business Associate to determine that the Breach is mitigated to the extent practicable.

5.4. Law Enforcement Delay. The Privacy Officer will assure that they, or the Business Associate, abide with Section 4.5.

5.5. Institutional Actions. Each Compliance or Privacy Officer will report all substantial Breach incidents as soon as practicable to the Corporate Vice President of Compliance and the MHC Chief Information Security Officer. All actual or potential breach incidents will be reported in the MHC quarterly compliance report.

5.5.1. MHC has the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of Unsecured PHI did not constitute a Breach. In order to demonstrate this evidence, the Privacy Officer will track all actual or potential Breach investigations, including Breaches by Business Associates, in Comply Track or similar tracking software as approved by the MHC Corporate Vice President of Compliance.

## 6. References

6.1. 45 CFR Parts 160 and 164

6.2. MCL 445.72 - IDENTITY THEFT PROTECTION ACT 452 of 2004, Notice of Security Breach, Requirements

6.3. Title XIII of the American Recovery and Reinvestment Act (ARRA), subtitled: Health Information Technology for Economic and Clinical Health Act (HITECH), including Subpart D – Privacy

6.4. MHC CC_0110 Record Retention Policy

6.5. MHC CC_0114 Non-Retaliation

6.6. MHC CC_0118 Identity Theft Prevention Program

6.7. MHC CC_1104 Joint Notice of Privacy Practices

6.8. MHC CC_1106 Business Associates

6.9. Notification to McLaren about a Security Incident and/or Breach of Unsecured Protected Health Information Form MHC_CC1106.7.4

6.10.

7. Appendix

7.1. Breach Discovery and Reporting Process

7.2. Breach Notification Decision Tree

7.3. a) MHC Breach Risk Assessment Tool; b) Business Associate Breach Risk Assessment Tool

7.4. Individual Notice Template

7.5. Media Notice Template

7.6. Notice to the Secretary Sample (must be completed online)

**Previous Revisions:** January 18, 2011, November 17, 2011, September 19, 2013, May 21, 2015, November 13, 2017, July 22, 2019

**Supersedes Policy:** Not Applicable

**Approvals:**

**HIPAA Council:** December 1, 2010, August 3, 2011, March 5, 2014, May 6, 2015, October 4, 2017, July 10, 2019, June 3, 2020, June 16, 2021, January 5, 2022

**Corporate Compliance Committee:** January 18, 2011, November 17, 2011, September 19, 2013, March 20, 2014, May 21, 2015, November 13, 2017, July 22, 2019, June 15, 2020, July 20, 2021, January 11, 2022

*Signature on File*
Gregory R. Lane
Sr. VP and Chief Administrative Officer

1/11/2022
Date