

		<b>Policy Title:</b>	HIPAA Administrative Policy
<b>Effective Date:</b>	January 20, 2011	<b>Policy Number:</b>	MHC_CC1105
<b>Review Date:</b>	December 14, 2015	<b>Section:</b>	Compliance
<b>Revised Date:</b>	September 18, 2014	<b>Oversight Level:</b>	Corporate
<b>Administrative Responsibility:</b>	Corporate Director of Compliance; HIPAA Council		

**1. Purpose**

1.1. This policy sets forth the Administrative structure that MHC is required to maintain in order to comply with the HIPAA Rules.

**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.

**3. Definitions**

3.1. **Business Associate** means an organization or a person, other than a Workforce Member who on behalf of MHC, creates, receives, maintains, or transmits PHI for:

3.1.1. claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; patient safety activities; billing; benefit management; practice management; and re-pricing; or

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

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

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

3.1.2.3. Provides personal health records to one or more individuals on behalf of MHC;

3.1.2.4. Is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the Business Associate;

3.1.3. Business Associate does not include:

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

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

**3.2. Electronic Protected Health Information (ePHI)** is PHI that is in electronic form (see definition for Protected Health Information).

**3.3. Health Plan** is a covered entity that receives health information electronically in connection with a covered transaction, such as accepting submitted health care claims from a health care provider.

**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. Incidental Use or Disclosure** is defined as a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure under the Privacy Rule.

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

**3.7. Notice of Privacy Practices (NPP)** is a notice of the uses and disclosures of protected health information that may be made by MHC, and of the individual's rights and MHC's legal duties with respect to protected health information.

**3.8. Payment** means the activities undertaken by a provider or health plan to obtain or provide reimbursement for the provision of health care. Activities related to the Individual to whom health care is provided and include, but are not limited to the following:

**3.8.1.** Determinations of eligibility or coverage;

**3.8.2.** Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing;

**3.8.3.** Review of services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.

**3.8.4.** Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and,

**3.8.5.** Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or payment:

**3.8.5.1.** Name and address;

**3.8.5.2.** Date of birth;

**3.8.5.3.** Social security number;

**3.8.5.4.** Payment history;

**3.8.5.5.** Account number; and

**3.8.5.6.** Name and address of the health care provider and/or health plan.

**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. PHI is any information that:

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

**3.9.2.** Relates to the provision of health care to an Individual.

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

**3.9.4.** 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, including, but not limited to: name, medical record number, encounter number, social security number, address, and photo, and 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.

**3.9.4.1.** PHI excludes:

**3.9.4.2.** 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);

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

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

**3.10. Treatment** means the provision, coordination or management of health care and related services by one or more providers, including the coordination or management of health care by a provider with a third party; consultation between providers relating to a patient; or the referral of a patient for health care from one provider to another.

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

**3.12. 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. Privacy**

###### **4.1.1. Personnel Designation**

**4.1.1.1.** MHC must designate a privacy official who is responsible for the development and implementation of the policies and procedures at each subsidiary organization.

**4.1.1.2.** MHC must designate a contact person or office who is responsible for receiving complaints under the Administrative Requirements and who is able to provide further information about matters covered by the NPP.

**4.1.1.3.** MHC must document the personnel designations as required by this policy.

#### **4.1.2. Training**

**4.1.2.1.** MHC must train all members of its Workforce on the policies and procedures required by the HIPAA Rules with respect to PHI, as necessary and appropriate for the members of the Workforce to carry out their functions within MHC.

#### **4.1.3. Safeguards**

**4.1.3.1.** MHC must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

**4.1.3.2.** MHC must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the requirements of the HIPAA Rules.

**4.1.3.3.** MHC must reasonably safeguard PHI to limit Incidental Uses or Disclosures made pursuant to an otherwise permitted or required Use or Disclosure.

#### **4.1.4. Complaints**

**4.1.4.1.** MHC must provide a process for Individuals to make complaints concerning MHC's policies and procedures, its compliance with such policies and procedures and/or the requirements of the HIPAA Rules.

**4.1.4.2.** MHC must document all complaints received, and their disposition, if any.

#### **4.1.5. Sanctions**

**4.1.5.1.** MHC must have and apply appropriate sanctions against members of its Workforce who fail to comply with its privacy policies and procedures or the requirements of the HIPAA Rules. This does not apply to Workforce Members with respect to actions that are covered by and that meet the conditions of the HIPAA Rules or this policy.

**4.1.5.2.** MHC must document the sanctions that are applied, if any, as required in this policy.

#### **4.1.6. Mitigation**

**4.1.6.1.** MHC must mitigate, to the extent practical, any harmful effect that is known of a Use or Disclosure of PHI in violation of its policies and procedures or the requirements of the HIPAA Rules by MHC or its Business Associate.

#### **4.1.7. Refraining from Intimidation or Retaliatory Acts**

**4.1.7.1.** See Policy MHC CC\_0114 Non Retaliation.

**4.1.7.2.** MHC may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for:

**4.1.7.2.1.** Exercising their right under, or for participation in any process established by the HIPAA Rules, including the filing of a complaint under this section;

**4.1.7.2.2.** Filing of a complaint with the Secretary under the HIPAA Rules;

**4.1.7.2.3.** Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the Regulation; or

**4.1.7.2.4.** Opposing any act or practice made unlawful by the HIPAA Rules, provided the Individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a Disclosure of PHI in violation of the HIPAA Rules.

#### **4.1.8. Waiver of Rights**

**4.1.8.1.** MHC may not require Individuals to waive their rights under the HIPAA Rules as a condition of the provision of Treatment, Payment, enrollment in a Health Plan, or eligibility for benefits.

#### **4.1.9. Policies and Procedures**

**4.1.9.1.** MHC must implement policies and procedures with respect to PHI that are designed to comply with the HIPAA Rules. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to PHI undertaken by MHC, to ensure such compliance.

#### **4.1.10. Changes to Policies and Procedures**

**4.1.10.1.** MHC must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the HIPAA Rules;

**4.1.10.2.** When MHC changes a privacy practice that is stated in the NPP and makes corresponding changes to its policies and procedures, it may make the changes effective for PHI that it created or received prior to the effective date of the NPP revision, if MHC has, in accordance with the HIPAA Rules, included in the NPP a statement reserving its right to make such a change in its privacy practices; or

**4.1.10.3.** MHC may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with this section.

**4.1.10.4. *Changes in Law.*** Whenever there is a change in law that necessitates a change to the MHC's policies or procedures, MHC must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the NPP, MHC must promptly make the appropriate revisions to the NPP in accordance with the HIPAA Rules. Nothing in this paragraph may be used by MHC to excuse a failure to comply with the law.

**4.1.10.5.** *Changes to Privacy Practices Stated in the NPP.* See MHC CC\_1104 Notice of Privacy Practices.

**4.1.10.6.** *Changes to Other Policies or Procedures.* MHC may change, at any time, a policy or procedure that does not materially affect the content of the NPP required by the HIPAA Rules, provided that:

**4.1.10.6.1.** The policy or procedure, as revised, complies with the HIPAA Rules; and

**4.1.10.6.2.** Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by this policy.

#### **4.1.11.** Documentation

**4.1.11.1.** MHC must maintain the policies and procedures provided for in written or electronic form;

**4.1.11.2.** If a communication is required by the HIPAA Rules to be in writing, maintain such writing, or an electronic copy, as documentation; and

**4.1.11.3.** If an action, activity, or designation is required by the HIPAA Rules to be documented, maintain a written or electronic record of such action, activity, or designation.

**4.1.11.4.** MHC must retain the documentation required by this policy for six years from the date of its creation or the date when it last was in effect, or according to the MHC Record Retention Schedule, whichever is later.

#### **4.1.12.** Group Health Plans

**4.1.12.1.** A Group Health Plan is not subject to the requirements in Sections 4.1.1 through 4.1.6 and 4.1.9, to the extent that:

**4.1.12.1.1.** The Group Health Plan provides health benefits solely through an insurance contract with a Health Insurance Issuer or an HMO; and

**4.1.12.1.2.** The Group Health Plan does not create or receive Protected Health Information, except for:

**4.1.12.1.2.1.** Summary Health Information; or

**4.1.12.1.2.2.** Information on whether the Individual is participating in the Group Health Plan, or is enrolled in or has dis-enrolled from a Health Insurance Issuer or HMO offered by the plan.

**4.1.12.1.3.** A Group Health Plan is subject to the documentation requirements only with respect to plan documents amended in accordance with the HIPAA Rules.

#### **4.1.13.** Business Associates

**4.1.13.1.** For those relationships that constitute a "Business Associate" relationship, MHC shall enter into appropriate written agreements with the Business Associate as defined by MHC CC1106 HIPAA Business Associate and Data Use Agreement Policy.

## **4.2. Security**

**4.2.1.** MHC must designate a security official who is responsible for the development and implementation of the policies and procedures at each subsidiary organization.

### **4.2.2. Workforce Security**

**4.2.2.1.** Implement policies and procedures to ensure that all members of the workforce have appropriate access to ePHI.

### **4.2.3. Implementation Specifications**

**4.2.3.1.** MHC must implement procedures:

**4.2.3.1.1.** For the authorization of Workforce Members who work with ePHI or in locations where it might be accessed;

**4.2.3.1.2.** To determine that the access of a Workforce Member to ePHI is appropriate.

**4.2.3.1.3.** To assure that access to ePHI is terminated when the employment of a Workforce Member ends or is adjusted for a change to an employment classification in which ePHI access is no longer appropriate.

### **4.2.4. Training.**

**4.2.4.1.** MHC must train all members of its Workforce on the policies and procedures required by the HIPAA Rules with respect to ePHI, as necessary and appropriate for the members of the Workforce to carry out their functions within MHC. At a minimum, this training must include:

**4.2.4.1.1.** Periodic security updates,

**4.2.4.1.2.** Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software.

**4.2.4.1.3.** Log-in monitoring. Procedures for monitoring log-in attempts and reporting discrepancies.

**4.2.4.1.4.** Password management. Procedures for creating, changing, and safeguarding passwords.

### **4.2.5. Security Incidents Procedures**

**4.2.5.1.** MHC will implement policies and procedures to address security incidents.

### **4.2.6. Response and Reporting**

**4.2.6.1.** MHC will identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to MHC; and document security incidents and their outcomes.

### **4.2.7. Contingency Plan**

**4.2.7.1.** MHC will establish policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.

**4.2.7.2. *Data backup plan.*** MHC will establish and implement procedures to create and maintain retrievable exact copies of ePHI.

**4.2.7.3. *Disaster recovery plan.*** MHC will establish, and implement as needed, procedures to restore any loss of data.

**4.2.7.4. *Emergency mode operation plan.*** MHC will establish, and implement as needed, procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

**4.2.7.5. *Testing and revision procedures.*** MHC will implement procedures for periodic testing and revision of contingency plans.

**4.2.7.6. *Applications and data criticality analysis.*** MHC will assess the relative criticality of specific applications and data in support of other contingency plan components.

#### **4.2.8. Evaluation**

**4.2.8.1.** MHC will perform a periodic technical and nontechnical evaluation in response to environmental or operational changes affecting the security of ePHI that establishes the extent to which MHC's security policies meet the requirements set forth in this policy.

#### **4.2.9. Business Associate Agreements and other arrangements**

**4.2.9.1.** MHC may permit a Business Associate to create, receive, maintain, or transmit ePHI on MHC's behalf only if MHC obtains satisfactory assurances that the Business Associate will appropriately safeguard the information.

**4.2.9.2.** Section 4.2.9 does not apply with respect to the transmission of ePHI:

**4.2.9.2.1.** By MHC to a health care provider concerning the treatment of an individual.

**4.2.9.2.2.** By the Health Plan to a plan sponsor, to the extent that the other HIPAA Rules are met.

**4.2.9.3.** MHC will document the satisfactory assurances required in the MHC Business Associate Agreement (see policy MHC CC\_1106 Business Associate and Data Use Agreement Policy).

### **5. Procedure**

#### **5.1. Designation of a Privacy Official and a Security Official**

**5.1.1.** MHC and its subsidiaries will each designate a privacy and security official. Such designation will be confirmed annually by each entity's Board of Trustees.

#### **5.2. Training**

**5.2.1.** MHC must provide training, as follows:



**5.2.1.1.** To each member of the MHC Workforce annually and to each new member of the Workforce within a reasonable period of time after the person joins MHC's Workforce; and

**5.2.1.2.** To each member of MHC's Workforce whose functions are affected by a material change in the policies or procedures required by the HIPAA Rules, within a reasonable period of time after the material change becomes effective.

**5.2.1.3.** MHC must document that the training has been provided.

### **5.3. Complaints**

**5.3.1.** Complaints shall be addressed by the privacy and/or security official. The contact information for the privacy official shall be printed on the NPP.

**5.3.2.** Complaints and/or security incidents will be documented in a password-protected database provided by MHC (ComplyTrack).

### **5.4. Sanctions**

**5.4.1.** Sanctions related to violations of the Privacy or Security rules shall be determined by each subsidiary. Each violation is to be evaluated on its own merits. Documentation of sanctions, and any other complaint resolution, shall be included in the ComplyTrack database.

### **5.5. Mitigation**

**5.5.1.** Mitigation of complaints shall be completed in accordance with HIPAA Rules and guidance provided by HHS. Notification to the affected Individuals and reporting of violations shall be provided in accordance with HIPAA Rules. Refer to MHC\_CC1109 HIPAA Privacy and Security Breaches, Notification, and Mitigation for further information.

### **5.6. Refraining from Intimidation or Retaliatory Acts**

**5.6.1.** Refer to policy MHC\_CC0114 Non-Retaliation Policy for guidelines related to intimidation or retaliation.

### **5.7. Business Associates**

**5.7.1.** MHC will document and execute Business Associate Agreements with its Business Associates in compliance with MHC CC1106 *HIPAA Business Associate and Data Use Agreement Policy*.

## **6. References**

**6.1.** MHC CC0106 Acceptable Use of Technology Resources Policy

**6.2.** MHC CC0110 Record Retention Policy

**6.3.** MHC CC0114 Non Retaliation Policy

**6.4.** MHC CC1104 Notice of Privacy Practices Policy

**6.5.** MHC CC1106 Business Associate and Data Use Agreement Policy

6.6. MHC CC1109 HIPAA Privacy and Security Breaches, Notifications, and Mitigation Policy

6.7. HHS Security HIPAA Rules Administrative Safeguards § 164.306

6.8. Subsidiary Contingency Plans

7. **Appendix:** Not applicable

**Previous Revisions:** January 20, 2011, September 18, 2014

**Supersedes Policy:** Subsidiary HIPAA Administrative Policies

**Approvals:**

**HIPAA Council:** May 5, 2010; January 5, 2011, August 7, 2014, October 7, 2015

**Corporate Compliance Committee:** January 20, 2011, September 18, 2014, December 14, 2015



---

Gregory L. Lane  
Sr. VP and Chief Administrative Officer

---

December 14, 2015  
Date