MCLaren HEALTH CARE		Policy Title:	HIPAA Privacy and Security Breaches, Notifications, and Mitigation	
HEALTH CARE				
Effective Date:	January 18, 20	011	Policy Number:	MHC_CC1109
Review Date:			Section:	Compliance
Revised Date:	June 16, 2021		Oversight Level:	Corporate
Administrative Responsibility: Corporat			e VP of Complianc	e; 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.
- **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.** <u>Additional Notice in Urgent Situations</u>. 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.** <u>Timing and Content of Notice</u>. 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 <a href="https://ocrportal.hhs.gov/ocr/breach">https://ocrportal.hhs.gov/ocr/breach</a> (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

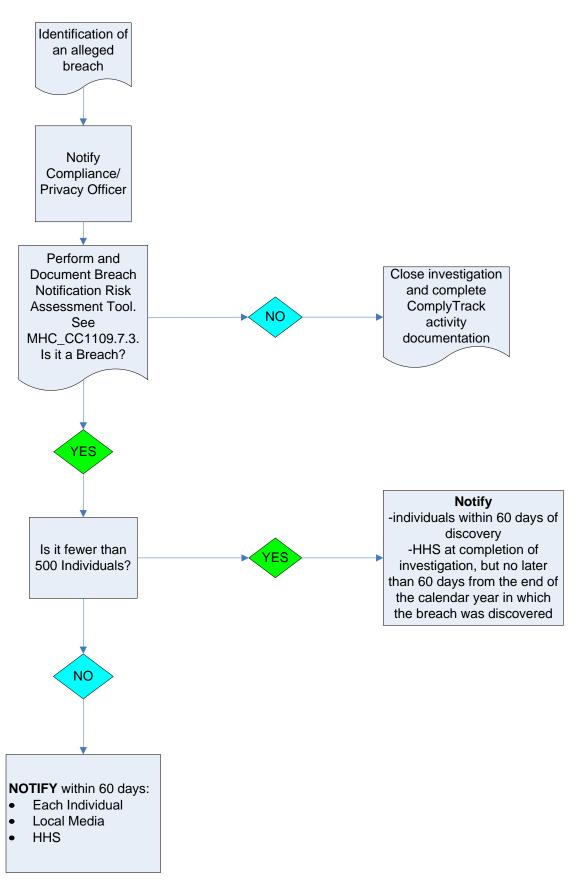
#### Approvals:

**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

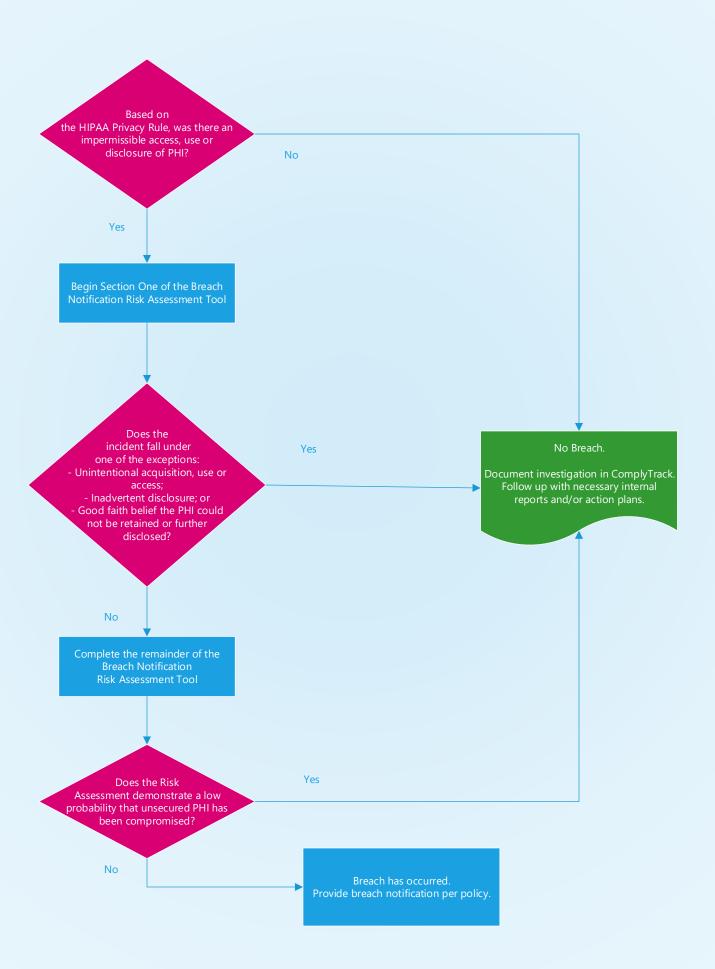
**Corporate Compliance Committee:** January 18, 2011, November 17, 2011, September 19, 2013, March 20, 2014, May 21, 2015, November 13, 2017, July 22, 2019, June 15, 2020, July 20, 2021

Signature on File	July 20, 2021
Gregory R. Lane	Date
Sr. VP and Chief Administrative Officer	

### **Breach Discovery and Reporting Process**



### **BREACH NOTIFICATION DECISION TREE**



Incident/Name	Date of Discovery:
Number of individuals effected by the breach and/or security incident (please attach a list to identify the individuals):	Email Address of Reporter:
Incident Reported By (Name/Title):	Phone # of Reporter:
<b>Type of Incident:</b> Please specify the type of privacy and/or security incident that occurred and details of the PHI involved below.	Check all that apply: ☐ Inappropriate Access of PHI
	☐ Inappropriate Disclosure of PHI
	☐ Inappropriate Use of PHI
<b>Source of Incident:</b> Who was responsible for the inappropriate access, use or disclosure?	☐ Workforce Member
	☐ Business Associate
	☐ Business Associate Subcontractor
	☐ Other Authorized User
	Other Unauthorized User (ex: theft, hacker)
Notification by Business Associate or Business Associate Subcontractor (Business Associate made us aware of incident)	BA Contact Name:
Miles to the DA/Ocethority O	Contact Email:
Who is the BA/Contractor?  In these an executed agreement in place with the BA/Contractor that	Contact Phone:
<ul> <li>Is there an executed agreement in place with the BA/Contractor that includes HIPAA provisions (such as a Business Associate Agreement)?</li> </ul>	Date Notified by BA:
When did the BA/Contractor notify the McLaren of the incident?	Date BA Discovered:
How was the McLaren notified of the incident?	
Are we the Business Associate?	☐ Yes
Enter the date that our organization became aware of the incident	☐ Not Applicable
If we are the Business Associate, enter the date we notified the other Covered Entity of the incident	Date of Discovery:  Date Covered Entity Notified:

Section 1	
Was data properly secured (e.g., encrypted, or secure or properly destroyed (shredded) in compliance with	
Notification Rule?	□ NO
If Yes, then STOP here. No breach has occurred that requ If No, then proceed to next question.	uires notification.
n no, then proceed to next question.	
2. Does this incident qualify as one of the following exc a. Good faith, unintentional acquisition, access of	· · · · · · · · · · · · · · · · · · ·
Member	of use of Frii by Workforce
<ul> <li>b. Inadvertent disclosure to another authorized p</li> </ul>	•
c. Recipient could not reasonably have retained	the data
If any checked, then STOP here. No breach has occurred the	•
If none apply, proceed to next section to continue the asses the breach poses more than a low probability of data comprrequire breach notification.	

If you did not hit a STOP above in Section 1, then work through the rest of the assessment to determine if the *breach poses more than a low probability of data compromise to the extent that it would require breach notification.* 

Go to Section 2

Check **all that apply** in each subsection and use highest applicable score:

		Section 2	
Va	riable	Options	Score
		☐ No evidence that data was accessed or disclosed	0
I.	Method of Disclosure	☐ Unauthorized internal acquisition, access and/or use without disclosure outside of organization	1
		<ul><li>□ Verbal Disclosure</li><li>□ View only</li></ul>	2
		☐ Paper / Fax ☐ Electronic (email, mobile media, archive media, PC, server, etc.)	3
		☐ No data accessed or disclosed	0
II.	Amount of Data	☐ Small amount – e.g., demographic information; limited data set; 1-10 individuals	1
		☐ Moderate volume – 11-100; portions of records; a bill or EOB with coded information	2
		☐ Large volume – over 100; unknown volume; archive or mobile media or device compromised; entire record, database with multiple fields of data	3

Data Acquired or Viewed  mited or Demographic Data Only mited Data Set (evaluate possibility of re-identification if ZIP Code ad/or DOB included) mly identifiers breached are not defined under MI Identity Theft otection Act, and no other health information is breached: name, address, city, state, telephone number, fax number, e-mail address, dmission/discharge dates, service dates, date of death  eneral PHI formation about treatment, diagnosis, service, medication, etc.  nancial Data and/or Personal Identifiers  Information defined by the MI Identity Theft Protection Act which includes the person's first name or first initial and last name in combination with any of the following:  Social security or employer taxpayer identification numbers  Driver's license, State identification card, or passport numbers	1 2 3
mited or Demographic Data Only mited Data Set (evaluate possibility of re-identification if ZIP Code ad/or DOB included) mly identifiers breached are not defined under MI Identity Theft rotection Act, and no other health information is breached: name, address, city, state, telephone number, fax number, e-mail address, amission/discharge dates, service dates, date of death  eneral PHI formation about treatment, diagnosis, service, medication, etc.  nancial Data and/or Personal Identifiers  Information defined by the MI Identity Theft Protection Act which includes the person's first name or first initial and last name in combination with any of the following: Social security or employer taxpayer identification numbers	2
mited Data Set (evaluate possibility of re-identification if ZIP Code ad/or DOB included)  mly identifiers breached are not defined under MI Identity Theft rotection Act, and no other health information is breached: name, address, city, state, telephone number, fax number, e-mail address, dmission/discharge dates, service dates, date of death  eneral PHI formation about treatment, diagnosis, service, medication, etc.  Information defined by the MI Identity Theft Protection Act which includes the person's first name or first initial and last name in combination with any of the following:  Social security or employer taxpayer identification numbers	2
formation about treatment, diagnosis, service, medication, etc.  nancial Data and/or Personal Identifiers  Information defined by the MI Identity Theft Protection Act which includes the person's first name or first initial and last name in combination with any of the following:  Social security or employer taxpayer identification numbers	
Information defined by the MI Identity Theft Protection Act which includes the person's first name or first initial and last name in combination with any of the following:  Social security or employer taxpayer identification numbers	3
Checking account numbers Savings account numbers Credit card numbers Debit card numbers Personal Identification (PIN) Code as defined in G.S. 14-113.8(6) Any other numbers or information that can be used to access a person's financial resources Passwords-if the information would provide access to financial information or resources Sensitive Protected Health Information which may include information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health Decify the Type(s) of Information Accessed or Disclosed:	
	Debit card numbers  Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)  Any other numbers or information that can be used to access a person's financial resources  Passwords-if the information would provide access to financial information or resources  Sensitive Protected Health Information which may include information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health

	Section 2	
Variable	Options	Score
	☐ Not applicable	0
IV. Who Received or Accessed the PHI	☐ A member of MHC Workforce ☐ Business Associate/Business Associate subcontractor ☐ Business Associate/Subcontractor Workforce ☐ Another Covered Entity	1
	<ul> <li>□ Wrong Payor (not the patient's)</li> <li>□ Unauthorized family member</li> <li>□ Non-healthcare organization</li> <li>□ Government agency</li> </ul>	2
	☐ Media ☐ Unknown/Lost/Stolen ☐ Member of the general public	3
	☐ Unintentional access to or disclosure of PHI	1
V. Circumstances of release	☐ Lost or unable to determine whether compromise was likely	2
Officials	<ul> <li>☐ Intentional disclosure w/o authorization</li> <li>☐ Intentional acquisition/use/access w/o authorization using false pretense to obtain or disclose</li> <li>☐ Obtained for personal gain/malicious harm</li> <li>☐ Hack</li> <li>☐ Theft – Device targeted or Data targeted</li> </ul>	3
VI. Disposition/ Mitigation (What happened to the information after the initial	<ul> <li>☐ Visual- viewed only with no further disclosure</li> <li>☐ Information returned complete</li> <li>☐ Information properly destroyed and attested to by workforce member, another covered entity or business associate</li> <li>☐ Data Wiped by remote application</li> <li>☐ Forensic analysis found no information accessed</li> </ul>	1
disclosure)	☐ Information properly destroyed (outside organization/individual) ☐ Information/Device is encrypted or protected with proprietary software, but does not meet compliance with NIST Standards ☐ Information Destroyed, but does not meet compliance with NIST Standards ☐ Password protected – password not compromised or unknown if password compromised	2
	<ul> <li>□ Password protected – password was compromised</li> <li>□ Data not encrypted, readable, but archived in a block format in no relational order. Password and proprietary system NOT required to view data.</li> <li>□ No known controls</li> <li>□ Unable to mitigate</li> <li>□ Unable to retrieve data</li> <li>□ Unsure of disposition or location</li> <li>□ Suspicion of pending re-disclosure</li> <li>□ PHI already re-disclosed</li> <li>[Continued on next page]</li> </ul>	3

☐ Sent to the Media		
SCORING		
Total Probability of Compromise So	CORE (Section 2)	
the scoring is meant to serve as a guide in your decision making you. There are a variety of factors and mitigations that may annot foresee or predict. An attempt was made to develop this is our actions, consider factors and circumstances and then aid otification or not making a breach notification.	be involved in your incident that a way that would help you in doo	at this too cumenting
Probability of Compro	omise	
Low	High	_
0 9		—- <b>►</b> 18
Additional information and basis for decision:	Final Decision	
	Low Probability of Compromise	
	Breach Requiring Notice	
Resolution and Corrective Action(s) (actions taken to prevent and target dates for completion):  Corrected system issues (e.g., disabled auto-faxing, updated Reviewed user security access levels for appropriateness and Changed or updated policies/procedures Discussed results with leader(s) and identified changes to in Counseled/educated to person or staff members to assure the Retrieved PHI or documented recipient's assurances that Physical Document in detail all the above corrective actions in Com	d system with correct information didentified required changes approve process or prevent reocchey understand what they did will was destroyed or not further of	n, etc.) currence as wrong
Complete this section if breach notific	cation is required:	
Date of Notice to Individual(s):		
Credit monitoring offered to individual:		
Date of Notice to Secretary HHS:		

Incident/Name	Date of Discovery:
Number of individuals effected by the breach and/or security incident (please attach a list to identify the individuals):	Email Address of Reporter:
Incident Reported By (Name/Title):	Phone # of Reporter:
<b>Type of Incident:</b> Please specify the type of privacy and/or security incident that occurred and details of the PHI involved below.	Check all that apply:  ☐ Inappropriate Access of PHI
	☐ Inappropriate Disclosure of PHI
	☐ Inappropriate Use of PHI
<b>Source of Incident:</b> Who was responsible for the inappropriate access, use or disclosure?	☐ Business Associate Workforce Member
	☐ Business Associate Subcontractor
	☐ Other Unauthorized User (ex: theft, hacker)
Notification by Business Associate or Business Associate Subcontractor (Business Associate made us aware of incident)	BA Contact Name:
Who is the BA/Contractor?	Contact Email:
	Contact Phone:
<ul> <li>Is there an executed agreement in place with the BA/Contractor that includes HIPAA provisions (such as a Business Associate Agreement)?</li> </ul>	Date BA Notified MHC:
, ig. 303) .	Date BA Discovered Incident:
<ul> <li>When did the BA/Contractor notify the McLaren of the incident?</li> </ul>	
<ul> <li>How was the McLaren notified of the incident?</li> </ul>	

Section 1	
[Section Removed]	
1. Was data properly secured (e.g., encrypted, or secured as specified in NIST guidance) or properly destroyed (shredded) in compliance with the requirements in the Breach Notification Rule?	☐ YES
Notification Rule?	□ NO
If Yes, then STOP here. No breach has occurred that requires notification.  If No, then proceed to next question.	
2. Does this incident qualify as one of the following exceptions? Check any that apply.	
a. Good faith, unintentional acquisition, access or use of PHI by Workforce	
Member	
b. Inadvertent disclosure to another authorized person within the entity or OHCA	
C. Recipient could not reasonably have retained the data	
If any checked, then STOP here. No breach has occurred that requires notification.  If none apply, proceed to next section to continue the assessment and determine if	
the breach poses more than a low probability of data compromise, to the extent that it would require breach notification.	

If you did not hit a STOP above in Section 1, then work through the rest of the assessment to determine if the *breach poses more than a low probability of data compromise to the extent that it would require breach notification.* 

Go to Section 2

Check **all that apply** in each subsection and use highest applicable score:

		Section 2	
Va	riable	Options	Score
I.	Method of	<ul><li>☐ No evidence that data was accessed or disclosed</li><li>☐ Attestation received that information was not further used or disclosed</li></ul>	0
	Disclosure	☐ Unauthorized internal acquisition, access and/or use without disclosure outside of organization	1
		<ul><li>□ Verbal Disclosure</li><li>□ View only</li></ul>	2
		☐ Paper / Fax ☐ Electronic (email, mobile media, archive media, PC, server, etc.)	3
		☐ No data accessed or disclosed	0
II.	Amount of Data	☐ Small amount – e.g., demographic information; limited data set; 1-10 individuals	1
		☐ Moderate volume – 11-100; portions of records; a bill or EOB with coded information	2
		☐ Large volume – over 100; unknown volume; archive or mobile media or device compromised; entire record, database with multiple fields of data	3

Section 2		
Variable	Options	Score
III. Noture and	☐ No Data Acquired or Viewed	0
III. Nature and Extent of PHI Involved	Limited or Demographic Data Only Limited Data Set (evaluate possibility of re-identification if ZIP Code and/or DOB included) Only identifiers breached are not defined under MI Identity Theft Protection Act, and no other health information is breached: name, address, city, state, telephone number, fax number, e-mail address, admission/discharge dates, service dates, date of death	1
	☐ General PHI  Information about treatment, diagnosis, service, medication, etc.	2
	<ul> <li>Financial Data and/or Personal Identifiers</li> <li>Information defined by the MI Identity Theft Protection Act which includes the person's first name or first initial and last name in combination with any of the following:</li> <li>Social security or employer taxpayer identification numbers</li> <li>Driver's license, State identification card, or passport numbers</li> <li>Checking account numbers</li> <li>Savings account numbers</li> <li>Credit card numbers</li> <li>Debit card numbers</li> <li>Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)</li> <li>Any other numbers or information that can be used to access a person's financial resources</li> <li>Passwords-if the information would provide access to financial information or resources</li> <li>Sensitive Protected Health Information which may include information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health</li> </ul>	3
	Specify the Type(s) of Information Accessed or Disclosed:	

Section 2			
Variable	Options	Score	
	☐ Not applicable	0	
IV. Who Received or Accessed the PHI	☐ A member of MHC Workforce ☐ Business Associate/Business Associate subcontractor ☐ Business Associate/Subcontractor Workforce ☐ Another Covered Entity	1	
	<ul> <li>□ Wrong Payor (not the patient's)</li> <li>□ Unauthorized family member</li> <li>□ Non-healthcare organization</li> <li>□ Government agency</li> </ul>	2	
	☐ Media ☐ Unknown/Lost/Stolen ☐ Member of the general public	3	
	☐ Unintentional access to or disclosure of PHI	1	
V. Circumstances of release	☐ Lost or unable to determine whether compromise was likely	2	
Orrelease	<ul> <li>☐ Intentional disclosure w/o authorization</li> <li>☐ Intentional acquisition/use/access w/o authorization using false pretense to obtain or disclose</li> <li>☐ Obtained for personal gain/malicious harm</li> <li>☐ Hack</li> <li>☐ Theft – Device targeted or Data targeted</li> </ul>	3	
VI. Disposition/ Mitigation (What happened to the information after the initial	<ul> <li>☐ Visual- viewed only with no further disclosure</li> <li>☐ Information returned complete</li> <li>☐ Information properly destroyed and attested to by workforce member, another covered entity or business associate</li> <li>☐ Data Wiped by remote application</li> <li>☐ Forensic analysis found no information accessed</li> </ul>	1	
disclosure)	☐ Information properly destroyed (outside organization/individual) ☐ Information/Device is encrypted or protected with proprietary software, but does not meet compliance with NIST Standards ☐ Information Destroyed, but does not meet compliance with NIST Standards ☐ Password protected – password not compromised or unknown if password compromised	2	
	<ul> <li>□ Password protected – password was compromised</li> <li>□ Data not encrypted, readable, but archived in a block format in no relational order. Password and proprietary system NOT required to view data.</li> <li>□ No known controls</li> <li>□ Unable to mitigate</li> <li>□ Unable to retrieve data</li> <li>□ Unsure of disposition or location</li> <li>□ Suspicion of pending re-disclosure</li> <li>□ PHI already re-disclosed</li> </ul>	3	

	Sent to the Media	isk /\ssc35\text{\tinx}\text{\ti}\xititet{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\ti}\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\tex{\tex		
	SCORING			
Total Pro	obability of Compromise Sco	ore (Section 2)		
or you. There are a va annot foresee or predi our actions, consider	o serve as a guide in your decision making ariety of factors and mitigations that may be ct. An attempt was made to develop this is a factors and circumstances and then aid in ng a breach notification.	e involved in your incident that way that would help you in doc	this tool umenting	
	Probability of Comprom			
4	Low	High	<b>_</b>	
0	9		18	
Additional informati	on and basis for decision:	Final Decision		
		Low Probability of Compromise		
		Breach Requiring Notice		
Resolution and Corrective Action(s) (actions taken to prevent recurrence, responsible individual(s), and target dates for completion):				
<ul> <li>□ Corrected system issues (e.g., disabled auto-faxing, updated system with correct information, etc.)</li> <li>□ Reviewed user security access levels for appropriateness and identified required changes</li> <li>□ Changed or updated policies/procedures</li> <li>□ Discussed results with leader(s) and identified changes to improve process or prevent reoccurrence</li> <li>□ Counseled/educated to person or staff members to assure they understand what they did was wrong</li> <li>□ Retrieved PHI or documented recipient's assurances that PHI was destroyed or not further disclosed</li> </ul>				
Document in detail a	all the above corrective actions in Comply	yTrack.		
	Complete this section if breach notifica	tion is required:		
Date of Notice to Individual(s):				
Credit monitoring offered to individual:				
Date of Notice to Secretary HHS:				
	ng Risk Assessment	 Date		

MHC\_CC1109.7.3b\_ BA Breach Risk Assessment Tool

Page **5** of **5** 

MHC\_CC1109.7.4 Individual Notice Template

**INSRT LOGO** 

To Enroll, Please Call: 1-800-939-4170

Or Visit: https://app.myidcare.com/account-creation/protect

Enrollment Code: [XXXXXXXXX]

Date

[Name] [Address] [City, State Zip]

#### Notice of Data Breach

Dear [Name],

[name of MHC entity] values your trust and confidence in us, and we are committed to securing our information systems and your protected health information.

#### What Happened

We recently learned on [insert event description and dates here].

#### What Information Was Involved

Example: The account information included name, date of birth, home address, phone number, account number and admit reason

#### What We Are Doing

Example: We have implemented additional safeguards to improve data security on our web server infrastructure.

#### What You Can Do

Due to this incident, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare<sup>™</sup>. With this protection, MyIDCare will help you resolve issues if your identity is compromised. We strongly encourage you to register for this free identity theft protection service. To enroll please visit <a href="https://app.myidcare.com/account-creation/protect">https://app.myidcare.com/account-creation/protect</a> or call 1-800-939-4170 and provide the following membership enrollment code: [Enrollment Code].

Your 12 month MyIDCare membership will include the following:

#### **Credit Monitoring and Recovery Services**

- **Single-Bureau Credit Monitoring -** Monitors any changes reported by Experian to your credit report.
- Access to the ID Experts Team Access to an online resource center for up-to-date information on new identity theft scams, tips for protection, legislative updates and other topics associated with maintaining the health of your identity.

MHC\_CC1109.7.4 Individual Notice Template

**INSRT LOGO** 

To Enroll, Please Call: 1-800-939-4170

Or Visit: https://app.myidcare.com/account-creation/protect

Enrollment Code: [XXXXXXXX]

- **Complete Recovery Services** Should you believe that you are a victim of identity theft, MyIDCare will work with you to assess, stop, and reverse identity theft issues.
- **Identity Theft Insurance** In the event of a confirmed identity theft, you may be eligible for reimbursement of up to \$1,000,000 for expenses related to that theft.

We sincerely regret any inconvenience or concern that this matter may have caused you. Thank you for your patience and understanding while we work together to protect you and your good name.

Sincerely,

Name
Title
[name of MHC entity]
Address

(Enclosure)

**INSRT LOGO** 

To Enroll, Please Call: 1-800-939-4170

Or Visit: https://app.myidcare.com/account-creation/protect

Enrollment Code: [XXXXXXXX]



#### **Recommended Steps to help Protect your Information**

Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore, credit monitoring may not be applicable at this time for them. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

- 1. Website and Enrollment. Go to <a href="www.idexpertscorp.com/protect">www.idexpertscorp.com/protect</a> and follow the instructions for enrollment using your Enrollment Code provided above. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the MyIDCare Member Website where you will find other valuable educational information.
- **2. Activate the credit monitoring** provided as part of your MyIDCare membership. Credit Monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- **3. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to <a href="https://www.annualcreditreport.com">www.annualcreditreport.com</a> or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**4. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any

**INSRT LOGO** 

To Enroll, Please Call: 1-800-939-4170

Or Visit: <a href="https://app.myidcare.com/account-creation/protect">https://app.myidcare.com/account-creation/protect</a>

Enrollment Code: [XXXXXXXX]

new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

#### **Credit Bureaus**

Equifax Fraud Reporting 1-800-525-6285 P.O. Box 740256 Atlanta, GA 30374-0241 www.alerts.equifax.com Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000

www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

- **5. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to \$5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.
- **6. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection, <a href="www.privacy.ca.gov">www.privacy.ca.gov</a>, for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, <a href="www.ag.ky.gov">www.ag.ky.gov</a>, Telephone: 1-502-696-5300.

**Maryland Residents**: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, <a href="www.oag.state.md.us/Consumer">www.oag.state.md.us/Consumer</a>, Telephone: 1-888-743-0023.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center

Raleigh, NC 27699-9001, <a href="https://www.ncdoj.com/">www.ncdoj.com/</a>, Telephone: 1-919-716-6400.

**INSRT LOGO** 

To Enroll, Please Call: 1-800-939-4170

Or Visit: https://app.myidcare.com/account-creation/protect

Enrollment Code: [XXXXXXXX]

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, <a href="www.riag.ri.gov">www.riag.ri.gov</a>, Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <a href="https://www.consumer.ftc.gov/">https://www.consumer.ftc.gov/</a>, 1-877-IDTHEFT (438-4338), 1-866-653-4261 (TTY)

### Call this number if you need language assistance: (###) ###-####

#### Spanish

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística.

#### Arabic

ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم

#### Chinese

注意:如果您使用繁體中文,您可以免費獲得語言援助服務。請致電

#### Vietnamese

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn.

#### Albanian

KUJDES: Nëse flitni shqip, për ju ka në dispozicion shërbime të asistencës gjuhësore, pa pagesë.

#### Korean

주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다.

#### Bengali

ল⊔য্ করনঃ যিদ আপিন বাংলা, কথা বলেত পােরেন, তাহেল িনঃখরচায় ভাষা সহায়তা পিরেষবা উপল আছে। েফান করন ১

#### Polish

UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej.

#### German

ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung.

MHC\_CC1109.7.4 Individual Notice Template

**INSRT LOGO** 

To Enroll, Please Call: 1-800-939-4170

Or Visit: https://app.myidcare.com/account-creation/protect

Enrollment Code: [XXXXXXXXX]

#### Italian

ATTENZIONE: In caso la lingua parlata sia l'italiano, sono disponibili servizi di assistenza linguistica gratuiti.

#### Japanese

注意事項:日本語を話される場合、無料の言語支援をご利用いただけます。

#### Russian

ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода.

#### Serbo-Croatian

OBAVJEŠTENJE: Ako govorite srpsko-hrvatski, usluge jezičke pomoći dostupne su vam besplatno.

#### **Tagalog**

PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad.

#### French

ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement.

Sample Media Notification Statement/Release - Document to be Reviewed and Customized Prior to Use.

#### [Insert Date]

**Contact:** [Insert Contact Information Including Phone Number/E-Mail Address]

**IMMEDIATE RELEASE** 

### [INSERT NAME OF ORGANIZATION] NOTIFIES PATIENTS OF BREACH OF UNSECURED PERSONAL INFORMATION

[Insert Name of Organization] notified [Insert Number] patients of a breach of unsecured personal patient protected health information after discovering the following event:

Describe event and include the following information as communicated to the victims:

- A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- B. A description of the types of unsecured protected health information that were 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 were involved).
- C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

In conjunction with local law enforcement and security experts, [Name of Organization] is working to notify impacted patients to mitigate the damages of the breach. [Name of Organization] has in place safeguards to ensure the privacy and security of all patient health information. As a result of this breach, steps are underway to further improve the security of its operations and eliminate future risk.

In a notification to patients, [Name of Organization] has offered their resources as well as .... [Insert as Applicable]. [Name of Organization] also has encouraged its

patients to contact their financial institutions to prevent unauthorized access to personal accounts.

[Name of Organization] has trained staff available for patients to call with any questions related to the data breach. Patients may call [Insert Phone Number Here] from [Insert Hours] with any questions. In addition, patients may visit [Name of Organization's] Web site at [Insert Web Address] for further information.

[Name of Organization] understands the importance of safeguarding our patients' personal information and takes that responsibility very seriously," said [Insert Name], President and CEO. "We will do all we can to work with our patients whose personal information may have been compromised and help them work through the process. We regret that this incident has occurred, and we are committed to prevent future such occurrences. We appreciate our patients support during this time.

Please direct all questions to [Enter Contact Information].

This document was generated by HIPAA Collaborative of Wisconsin. A copy of this document is free on their website at <a href="https://www.hipaacow.org">www.hipaacow.org</a>.

#### **Skip Navigation**

U.S. Department of Health & Human Services



Improving the health, safety, and well-being of America

Search

Font Size -+

Search OCR All HHS

Print Download Reader

HHS Home|HHS News|About HHS

# Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information

Breach Affecting  500 or More Individuals  Less Than 500 Individuals				
Report Type	Report Type			
O Initial Breach Report O Addendum to Previous Report				
Section 1 - Covered Entity				
Name of Covered Entity:	John Doe	Contact Name:	John Doe	
Address:	Line 1	Contact Phone Number: XXX-XXX-XXXX Contact E-mail:	xxx-xxxx example@example.com	
City: State: AL •	City  Zipcode: XXXX	Type of Covered Entity:	Health Plan	

### Section 2 - Business Associate Complete this section if breach occurred at or by a Business Associate

Name of Business Associate:	John Doe	Business Associate Contact Name:	John Doe
Address:	Line 1	Business Associate Contact Phone Number: XXX-XXXX	XXX-XXX-XXXX
	Line 2	Business Associate Contact E-mail:	example@example.com
City:	City		

ocrnotifications.hhs.gov 1/4

State: AL

Zipcode: xxxx

### **Section 3 - Breach**

Date(s) of Breach: MM/DD/YYYY mm/dd/yyyy - mm/dd/yyyy (-MM/DD/YYYY) Approximate Number of Individuals Affected by the Breach: Type of Breach: Theft Please select the Loss type of breach. If ■ Improper Disposal type breach is

Date(s) of Discovery: MM/DD/YYYY mm/dd/yyyy - mm/dd/yyyy (-MM/DD/YYYY)

Type of Breach (Other):

Location of Breached Information: Please select the location of the

"Other", please

describe the type

of breach in the

field below.

information at the time of the breach. If breach type is "Other", please describe the location of the information in more detail in the Description

Laptop **Desktop Computer** Network Server E-mail Other Portable Electronic Device Other

☐ Unauthorized Access/Disclosure

Hacking/IT Incident

Unknown

Other

Type of Protected Health Information Involved in the Breach:

section below.

Demographic Information Financial Information Clinical Information Other

**Brief Description** of the Breach:

ocrnotifications.hhs.gov 2/4

### Section 4 - Notice of Breach and Actions Taken

Date(s) Individual Notice Provided: mm/dd/yyyy - mm/dd/yyyy MM/DD/YYYY (- MM/DD/YYYY) O Yes O No Was Substitute Notice Required? O Yes O No Was Media Notice Required? Security and/or Privacy Safeguards Mitigation Actions Taken in Response to Breach: Sanctions Please select the actions taken to respond to the breach. If selecting the "Other" Policies and Procedures category, please describe the actions taken in the section below. Other Describe Other Actions Taken:

Please describe in detail any actions taken following the breach in addition to those selected above.

### **Section 5 - Attestation**

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as

ocrnotifications.hhs.gov 3/4

#### Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information

permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

Name:	Full Name	Date:	mm/dd/yyyy

Typing your name represents your signature

MM/DD/YYYY

Submit

HHS Home | Questions? | Contacting HHS | Accessibility | Privacy Policy | FOIA | Disclaimers | Inspector General | No FEAR Act | Viewers & Players

The White House | USA.gov | HHS Archive | Pandemic Flu

Washington, A CONTRIBUTE ON THE CONTRIBUTE ON TH U.S. Department of Health & Human Services • 200 Independence Avenue, S.W. • Washington, D.C. 20201

4/4 ocrnotifications.hhs.gov