Breach Notification Policy - Unsecured Protected Health Information

1. SCOPE

1.1 System-wide

1.2 Facilities and departments included in the scope are further defined in the Scope Definitions Resource Guide if not specifically outlined above.

2. DEFINITIONS & EXPLANATIONS OF TERMS

2.1. Abbreviations

- ARRA: American Recovery and Reinvestment Act
- HHS: Department of Health & Human Services
- HITECH: Health Information Technology for Economic and Clinical Health
- HIPAA: Health Insurance Portability and Accountability Act
- MCHS: Marshfield Clinic Health System
- PHI: Protected Health Information

2.2. Definitions

- Patient: All references to the "patient" in this policy mean the patient or her/his Personal Representative as defined in the Personal Representatives of Patients policy.
- Breach: Generally, is an impermissible use or disclosure under the HIPAA/HITECH Privacy & Security Rule that compromises the security or privacy of the Protected Health Information. Breach includes:
  - ◊ Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity or 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 under the Privacy Rule.
  - ◊ Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity's or Business Associate's facility to another person authorized to access PHI at the same facility, 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 under the Privacy Rule.
  - ◊ 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.
- Disclosure: The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Live
POLICY

- Risk assessment: Determines the probability that the Protected Health Information has been compromised.
- Privacy Rule: Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- Business Associate: A person or entity that performs certain functions or activities that involve the use or disclosure of Protected Health Information on behalf of, or provides services to, a covered entity.
- Covered Entity: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.
- Protected Health Information (PHI): The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information Protected Health Information.
    - ◊ Individually identifiable health information: information, including demographic data, that relates to:
        - the individual's past, present, or future physical or mental health or condition; **or**
        - the provision of health care to the individual; **or**
        - the past, present, or future payment for the provision of health care to the individual; **and**
        - that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual (e.g., name, address, birth date, Social Security Number).
- Unsecured Protected Health Information: Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. See Office for Civil Rights Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

Live
POLICY

3. POLICY BODY

Purpose Statement: Breach notification will be carried out by MCHS in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law. It is the purpose of this policy to establish guidelines for the notification of breaches of unsecured Protected Health Information to patient and the Office for Civil Rights.

3.1. Reporting of Breach: All suspected or potential breaches of PHI will be reported upon discovery and in a timely fashion to the Privacy Officer or Hospital Compliance Officer, depending on the setting of the breach. Reporting of a potential PHI breach can be accomplished via RL Incident Reporting or other notification methods available from the Corporate Compliance intranet site. When a breach involves printed PHI, every effort should be made to retrieve the original PHI that was sent/handed/faxed in error as quickly as possible. A self-addressed stamped envelope should be mailed to the unintended recipient to request return of the PHI. The preference is for MCHS to obtain the misdirected PHI from the unintended recipient.

3.2. Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to MCHS or by exercising reasonable diligence would have been known to MCHS (includes breaches by MCHS's Business Associates). MCHS shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (Business Associate) of MCHS. Following the discovery of a potential breach, MCHS shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach. MCHS shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

3.3. Breach Investigation: MCHS's Privacy Officer or Hospital Compliance Officer (depending on the setting in which the breach occurred) shall investigate the breach and shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in MCHS as appropriate (e.g., administration, human resources, risk management, marketing, legal counsel, etc.) The Privacy Officer or Hospital Compliance Officer shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.).

3.4. Risk Assessment: For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals or the HHS secretary under breach

Live
POLICY

notification requirements, MCHS must perform a risk assessment to determine probability that the individual's Protected Health Information has been compromised as a result of impermissible use or disclosure. MCHS shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. MCHS has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, MCHS will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

a. The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification.

b. The unauthorized person who used the Protected Health Information or to whom the disclosure was made.

c. Whether the Protected Health Information was actually acquired or viewed.

d. The extent to which the risk to the Protected Health Information has been mitigated.

3.5. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made to the patient without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by MCHS or the Business Associate involved. It is the responsibility of MCHS to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

3.6. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to MCHS that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, MCHS shall:

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

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

3.7. Content of the Notification: The notice shall be written in plain language and must contain the following information:

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 type of unsecured Protected Health Information disclosed in the breach (e.g., whether full name, Social Security Number, date of birth, home address, account number, diagnosis or other type of information was disclosed).

Live POLICY

c. Any steps the individual should take to protect themselves from potential harm resulting from the breach.

d. A brief description of what MCHS 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, website, or postal address.

f. During the notification process, every effort will be made to protect the confidentiality of anyone involved in the breach.

3.8. Methods of Notification: The method of notification will depend on the individuals/ entities to be notified. The following methods must be utilized accordingly:

a. Notice to Individual(s): Notice shall be provided promptly and in the following form:

- Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If MCHS knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out.
- Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, e-mail address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided 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.
  - In a case in which there is insufficient or out-of-date contact information for fewer than ten individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
  - In the case in which there is insufficient or out-of-date contact information for ten or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.
- If MCHS determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

b. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects 500 or

POLICY

more individuals. The Notice shall be provided in the form of a press release. The Privacy Officer will coordinate communication with the Marketing department.

c. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as noted below. The Secretary shall make available to the public on the HHS Internet website a list identifying Covered Entities involved in all breaches in which the unsecured PHI of 500 or more individuals is accessed, acquired, used, or disclosed.

   - For breaches involving 500 or more individuals, MCHS shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
   - For breaches involving less than 500 individuals, MCHS will maintain documentation (e.g., a log) for each breach. MCHS must annually submit details of each individual breach to the Secretary of HHS during the calendar year in which the breach occurred or no later than 60 days after the end of that same calendar year. Instructions for reporting individual breaches to HHS are provided at www.hhs.gov.

d. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, MCHS shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of individuals affected. The following information should be collected/logged for each breach:

   - A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known.
   - A description of the types of unsecured Protected Health Information disclosed in the breach (e.g., full name, Social Security Number, date of birth, home address, account number, etc.).
   - A description of the actions taken to notify any affected individuals that a breach occurred.
   - Resolution; steps taken to mitigate the breach and prevent future occurrences.

3.9. Business Associate Responsibilities: A Business Associate of MCHS that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured Protected Health Information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify MCHS of such breach. Such notice shall include the identification of each individual whose unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such breach. The Business Associate shall provide MCHS with any other available information that MCHS is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the Business Associate of discovery of a breach, MCHS will be responsible for notifying affected individuals, unless otherwise agreed upon by the Business Associate to notify the affected individuals.

Live POLICY

3.10. Workforce Training: As part of training to MCHS workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities, workforce members will be trained as to how to identify and report breaches within MCHS.

Live
POLICY

4. ADDITIONAL RESOURCES

4.1. References:

- HIPAA Regulation 45 CFR 164.404 – Notification to Individuals
- 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules
- 45 CFR 164.502(a)(1)(iii)
- Overview of Privacy Compliance Program
- HIPAA Privacy Definitions
- RL Incident Reporting
- Mitigation of Improper Uses and Disclosures

4.2. Additional Resources

- Office for Civil Rights Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.
- MCHS Data Security Incident Preparedness
- Reporting Misconduct

4.3. Applicable Procedures

- Reportable Breaches from all PFS Contracted Business Associates
- Suspected Privacy Breaches/PFS Customer Service

Live
POLICY

5. DOCUMENT HISTORY

Version No.	Revision Description
1.0	Policy #3500 converted to the New Document Control System
2.0	Minor changes: Updated the definition of "breach". Additional sentence to section 3.8.b.
3.0	Minor Changes: Addition to section 3.1, send a self-addressed stamped envelope to retrieve the PHI or confirm destruction of PHI. Addition of the definition of PHI and Unsecured PHI.
4.0	Updated Scope and MC to MCHS. Added templates to Additional Resources.
5.0	Updated Scope and Definitions. Added Applicable Procedures. Added 3.7.f and an Additional Resource.
6.0	Updated Scope and added Return of PHI Request Template. Updated formatting, metadata fields, header, removed logo, added abbreviations, updated author Adding Reporting Misconduct link updated HIPAA Privacy Definitions link
7.0	Annual review. Changed RL Solutions to RL Incident Reporting.
8.0	45 CFR 164.502(a)(1)(iii) reference added.
9.0-13.0	Refer to Version History
14.0	Administrative Override: Updated typo in 4.2.
15.0	Annual review. Updated broken link for RL Solutions.
16.0	Updated Section 3.1.
17.0	Updated templates under Section 4.2 to published links.
18.0	Updated CFR 164.404 link under Section 4.1.
19.0	Added "Mitigation of Improper Uses and Disclosures" to References.
20.0	DCS Checklist, AO to republish
21.0	Removed links to Return of PHI Request Template, AO to republish
22.0	Removed link to Individual Breach Notice template, AO to republish
23.0	Annual review, updated typo, added Lisa Lobner as approver

Live POLICY

6. DOCUMENT PROPERTIES

Primary Author: Schilling, Stacy
Co-Author(s): Lobner, Lisa G.
Approver(s): This document has been electronically signed and approved by: Lobner, Lisa G on: 4/7/2022 12:37:29 PM
This document has been electronically signed and approved by: Schilling, Stacy on: 4/7/2022 1:11:08 PM
This document has been electronically signed and approved by: Andrew, Donna J. on: 4/7/2022 1:27:32 PM

Live
POLICY