Breach Notification Policy (HIPAA)

Myra EB Systems

HIPAA: 45 CFR Part 164, Subpart D (§§ 164.400 - 164.414)

Keywords: Breach Notification Rule, Breach, Notification, Risk Assessment, Sanctions, Complaint Procedure

---

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that covered entities notify individuals whose unsecured protected health information has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the protected health information. In certain circumstances, a breach must also be reported to the Secretary of Health and Human Services (HHS) and through the media. The notification requirements only apply to breaches of *unsecured PHI*. In other words, if PHI is encrypted or destroyed in accordance with the HIPAA guidance, there is a "safe harbor" and notification is not required.

Purpose

This policy specifies the responsibilities, requirements, and procedures of Myra EB Systems in the event of a breach of unsecured PHI, as defined by 45 CFR Part 164, Subpart D (HIPAA "Breach Notification Rule").

Definitions

Breach. The acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted under the HIPAA Breach Notification Rule, which compromises the security or privacy of the protected health information. Breach excludes:

- Any unintentional acquisition, access, or use of protected health information 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 HIPAA.
- Any inadvertent disclosure by a person who is authorized to access PHA 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 under HIPAA.
- 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.

Business Associate. An entity, not a member of the Covered Entity's workforce, who:

- Performs or assists in performing a function or activity regulated by HIPAA, on behalf of a covered entity, involving the creation, receipt, maintenance, or transmission (i.e., use and disclosure) of PHI (including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing); or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI;
- Business Associates include:
- A health information organization;
- An e-prescribing gateway;
- Any entity that provides data transmission services with respect to PHI to a covered entity and that requires routine access to PHI;
- An entity that maintains PHI for a covered entity, whether or not the entity actually reviews the PHI.

Covered Entity. An entity that is:

- A health plan;
- A health care clearinghouse; or
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Protected Health Information (PHI). Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Unsecured Protected Health Information (Unsecured PHI). Any PHI which is not unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the HSS Secretary.

Workforce. Employees, volunteers, trainees, and other persons under the **direct control** of Myra EB Systems, whether or not they are paid by Myra EB Systems.

Scope

Myra EB Systems is a business entity that is considered to be a **<Select all applicable: COVERED ENTITY, HEALTH CLEARING HOUSE, BUSINESS ASSOCIATE>** with respect to protected health information (PHI), as provided by the standards, requirements, and implementation specifications of HIPAA Breach Notification Rule. Therefore, this policy applies to Myra EB Systems and all the members of its workforce with access to PHI. Additionally, all third parties, subcontractors, or vendors, that provide services to Myra EB Systems that involve the creation, receipt, maintenance, or transmission of private health information on behalf of the Employer to fulfill its contractual duties, must comply fully with HIPAA's requirements.

Roles and Responsibilities

<APPLICABLE ROLES & RESPONSIBILITIES RELATED TO REPORTING AND NOTIFICATION>

Policy and Procedures

Breach Discovery

A breach will be treated as *discovered*:

- From the first day it becomes known to Myra EB Systems; or,
- By exercising reasonable diligence, would have been known to Myra EB Systems or any entity, other than the person committing the breach, who is a workforce member or agent of Myra EB Systems.

Myra EB Systems workforce members who believe that PHI has been used or disclosed in any way that compromises the security or privacy of that information will immediately notify:

- **<list all as appropriate: his/her supervisor, the Practice administrator, the privacy officer, other>**.

Post-Breach Discovery

Following the discovery of a potential breach, Myra EB Systems will:

- Begin an investigation;
- Conduct a risk assessment; and based on the risk assessment results,
- Begin the process of notifying each individual whose PHI has been, or is reasonably believed by Myra EB Systems to have been, accessed, acquired, used, or disclosed as a result of the breach;
- Begin the process of determining what notifications are required or should be made, if any, to the Secretary of the Department of Health and Human Services (HHS), media outlets, [optional: or law enforcement officials].

Breach Investigation

Myra EB Systems will designate an individual to act as the investigator of the breach [or list that individual here: e.g., privacy officer, security officer, risk manager, other].

The investigator shall be responsible for:

- The management of the breach investigation;
- Completion of the risk assessment; and,
- Coordinating with:
    - **<Others in the company as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel.)>**
- Facilitate the notification process to the Myra EB Systems workforce, all of whom are expected to assist management in the investigation upon request.

Risk Assessment

For breach response and notification purposes, a breach is presumed to have occurred unless Myra EB Systems can demonstrate that there is a low probability that the PHI has been compromised. The overall probability will be evaluated based on, at minimum, the following risk factors or more, in combination:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Consider:
    - Social security numbers, credit cards, financial data
    - Clinical detail, diagnosis, treatment, medications
    - Mental health, substance abuse, sexually transmitted diseases, pregnancy
- The unauthorized person who used the PHI or to whom the disclosure was made.
    - Does the unauthorized person have obligations to protect the PHI's privacy and security?
    - Does the unauthorized person have the ability to re-identify the PHI?
- Whether the PHI was actually acquired or viewed.
    - Does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?
- The extent to which the risk to the PHI has been mitigated.
    - Can the Practice obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed?

Myra EB Systems will conduct a risk assessment thoroughly and will complete it in good faith, with reasonable conclusions and outcomes. Based on the outcome, Myra EB Systems will determine the need to move forward with breach notification.

The breach investigator will document the risk assessment and the outcome of the risk assessment process. All documentation related to the breach investigation, including the risk assessment, will be retained for a minimum of six years.

Notification Timeliness

Upon determination of a breach, Myra EB Systems will provide notification of the breach to appropriate entities without delay and no later than 60 calendar days after the discovery of the breach.

Myra EB Systems or its Business Associates may delay notification to individuals, HHS, or the Media, if a law enforcement official states to Myra EB Systems or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, if:

- The statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
- The statement is made orally, document the statement, including the identify 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.

Content and Methods of Notification

Myra EB Systems's notice to affected individuals is written in plain language and contains the following information, as included in Myra EB Systems's breach notification letter (see Appendix A):

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured PHI that were involved in the breach (e.g., whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
- Any steps the individuals should take to protect themselves from potential harm resulting from the breach.

- A brief description of what Myra EB Systems is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, email address, website, or postal address.

The notification letter will be:

- Sent by first-class mail to:
  - The individual at the last known address of the individual; or,
  - The next of kin of affected individual, if Myra EB Systems is aware that the individual is deceased and has the address of the next of kin or personal representative of the individual; or,
- Sent by Electronic mail upon the individual's agreement, and if such agreement has not been withdrawn, by electronic mail.
- Provided in one or more mailings as information is available.

If there is insufficient or out-of-date contact information that precludes direct written or electronic notification:

- For an individual, a substitute form of notice reasonably calculated to reach the individual will be provided.
- For fewer than 10 individuals, a substitute notice may be provided by an alternative form of written notice, by telephone, or by other means.
- For 10 or more individuals, a substitute notice will be in the form of a conspicuous posting:
  - On the home page of Myra EB Systems's website for a period of 90 days; or,
  - In major print or broadcast media in Myra EB Systems's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

Notification to Affected Individuals

If Myra EB Systems determines that breach notification must be sent to affected individuals, Myra EB Systems's standard breach notification letter will be sent out to all affected individuals (see Appendix A), in accordance with this policy. Additionally,

- Myra EB Systems has the discretion to provide notification following an impermissible use or disclosure of PHI *without performing a risk assessment*.
- In addition to the required 60-day maximum notification timeframe, if Myra EB Systems determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate.
- Myra EB Systems is responsible and will demonstrate that all notifications are made as required, including evidence demonstrating the necessity of any delay.
- A copy of all patient correspondence shall be retained by Myra EB Systems in accordance with state law record retention requirements, or any other regulation.

Notification to the Secretary of Health and Human Services

In the event of a breach of unsecured PHI, Myra EB Systems will notify HHS in a manner specified on the HHS Breach Reporting site, based on the number of affected individuals:

- For 500 or more affected individuals,
  - HHS will be notified at the same time the affected individuals are notified.
  - Submitted on the HHS Office for Civil Rights Breach Portal.
- For fewer than 500 affected individuals,
  - Myra EB Systems will maintain a log of all breaches discovered during the preceding calendar year, to be submitted annually to the Secretary of HHS.
  - Notice will be made, no later than 60 days after the end of each calendar year.
  - Submitted on the HHS Office for Civil Rights Breach Portal.

Notification to the Media

In the event that a breach affects more than 500 residents of a state, Myra EB Systems will notify:

- Prominent media outlets serving the state and regional area;
- Without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach;
- In the form of a press release.

Business Associate Responsibilities

Myra EB Systems's business associates will notify Myra EB Systems of a breach of unsecured PHI, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach of unsecured PHI. The notice will include:

- The identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.
- Any other available information that the Practice is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available.

Unless otherwise agreed within a Business Associate Agreement, when a business associate notifies Myra EB Systems of discovery of a breach, Myra EB Systems will be responsible for notifying affected individuals. **<Clarify who is responsible for notification, cost of such, etc., if applicable>**

Breach Information Maintenance

Myra EB Systems will maintain a process to record or log all breaches of unsecured PHI, regardless of the number of patients affected or whether the breach was discovered by Myra EB Systems or a business associate. For every breach, the following information will be collected:

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
- A description of the types of unsecured protected health information that were involved in the breach (such as full name, social security number, date of birth, home address, account number, other).
- A description of the action taken with regard to notification of patients regarding the breach.
- Steps taken to mitigate the breach and prevent future occurrences.

Workforce Training

Myra EB Systems will train all members of its workforce on:

- Myra EB Systems's policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities; and,
- How to identify and report breaches within Myra EB Systems. [Describe how the Practice trains its workforce – frequency, means, other.]

Training will be conducted:

- **<Frequency>**
- **<Method/Means>**
- **<Additional Information>**

Complaints

Myra EB Systems provides a process for individuals to make complaints concerning Myra EB Systems's privacy policies and procedures or its compliance with such policies and procedures (see Appendix B). Individuals also have the right to complain about the processes laid out in this policy.

Sanctions

Members of Myra EB Systems's workforce who fail to comply with this policy will be subject to disciplinary action, up to and including termination.

Retaliation/Waiver

Myra EB Systems or any member of its workforce will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his or her privacy rights. Individuals shall not be required to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Burden of Proof

Myra EB Systems 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.

APPENDIX A
[Sample] Breach Notification Letter

[Date]
[Name of Affected Individual]
[Individual's Address]
[City, State, ZIP]

NOTICE OF DATA BREACH

Dear [Affected Individual Name],

We are sending this letter to you as part of our continuing commitment to your privacy, and to inform you of a recent data breach at Myra EB Systems. Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected individuals about the incident, and outlining some steps you may take to help protect yourself.

WHAT HAPPENED

On [Date of Discovery] we became aware that your private information may have been compromised. We believe the breach occurred on or about [Date the breach actually occurred] and involved [brief description of what happened, such as theft, loss of files in transit, hacker attack. AVOID A STATEMENT OF BLAME].

WHAT INFORMATION WAS INVOLVED

The private information that may have been compromised includes:

- [Insert what type of information was breached, such as name, address, social security number, medical information]

WHAT WE ARE DOING

We have taken a number of steps to investigate this breach and prevent any potential harm to you , including but not limited to:

- [Insert what you did or are doing to investigate the breach and mitigate harm, including reporting to law enforcement, if applicable].

WHAT YOU CAN DO

To protect yourself from harm, you may take additional steps, including: [you may choose to add/substitute others, including offering a free year of credit monitoring if the breach is significant]

- Registering a fraud alert with a credit bureau such as the ones listed here, and ordering your credit reports:
  - Experian: www.experian.com,
  - TransUnion: www.transunion.com
  - Equifax: www.equifax.com
- Monitor your bank and credit card statements

We understand that this may pose an inconvenience to you. We sincerely apologize and regret that this situation has occurred. Myra EB Systems is committed to protecting your personal information, and we want to assure you that we have policies and procedures to protect your privacy.

If you have any questions, or if there is anything that we can do to assist you, please contact us at [Designated Phone Number], [available days and times].

APPENDIX B
Procedure for Submitting Complaints

[Outline process/procedure]