Subject: Breach Notification For Protected Health Information

Department: All Department

Approved/Amended On:
Effective Date:

This policy/procedure supersedes all other policies/procedures of the same subject.

Purpose

The Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA) requires HIPAA covered entities to notify affected individuals of certain security breaches concerning their protected health information (PHI). To ensure that EMSA complies with the breach notification regulation provisions (Breach Rule) of the Privacy Rule, this policy outlines the procedures for investigation and proper notification.

Policy

In the case of a breach of unsecured PHI, the patient or their personal representative must be notified without unreasonable delay and in no case later than 60 days of discovering the breach.
A breach is considered discovered by a covered entity or business associate as of the first day on which the breach is known by the exercise of reasonable diligence. A covered entity is deemed to have knowledge when the breach is known or should have been known by a workforce member or agent of covered entity. A business associate is deemed to have knowledge of a breach when it is known or should be known by an employee, officer or other agent of the business associate. Business associates are required to report any breach to the covered entity without unreasonable delay and no later than 60 days of discovering the breach.

If a law enforcement official determines that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed in the same manner as provided under §164.528(a)(2) of title 45, Code of Federal Regulations.

As a covered entity, EMSA, must work to timely and accurately report any breach of unsecured PHI according to ARRA, and any and all other Federal and State regulations and interpretive guidelines promulgated thereunder. The documentation must be maintained related to the breach (e.g., notification letters) for a minimum of six (6) years.

Definitions

The following definitions apply to all patient privacy and security policies and procedures.

1. Breach – Unauthorized acquisition, access, use, or disclosure of unsecured, unencrypted PHI which compromises the security or privacy of such information and poses a significant risk of financial, reputational, or other harm to the individual. To determine if a breach has occurred, a risk assessment must be performed to determine if the security or privacy of the PHI has been compromised. Limited Data Sets (except those that exclude patient zip code and date of birth) are subject to the breach notification reporting requirements. The term 'breach' does not include:

a. Any unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a covered entity or business associate if:
    i. Such acquisition, access, or use was made in good faith and within the course and scope of authority; and
    ii. Such information is not further used or disclosed in a manner not permitted;
b. Any inadvertent disclosure by a person who is authorized to access PHI of the covered entity or business associate, or organized health care arrangement in which the covered entity participates; and any such information received as a result of such disclosure is not further used or disclosed in a manner not permitted; or
c. 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.

2. Protected Health Information (PHI) – Any oral, written or electronic individually-identifiable health information collected or stored. Individually-identifiable health information includes demographic information and any information that relates to past, present or future physical or mental condition of an individual.

3. Unsecured PHI – PHI that is not encrypted and rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services (HHS).

4. Additional Definitions – Refer to the HIPAA Privacy Standards, 45 CFR Parts 160.101 and 164.501, for additional definitions.

Procedure: Identification of Breach Requiring Notification

1. Identification of Possible Breach – If a workforce member become aware of a possible breach of unsecured PHI, then the workforce member must immediately report the incident to the Privacy Officer.

2. Review of Possible Breach Requiring Notification – The Privacy Officer and/or designee, upon receiving notice of an incident that is a possible breach of unsecured PHI, shall without delay review the facts and circumstances of the possible breach in light of the Breach Rule exceptions and analyze whether sufficient harm to affected individuals has occurred so as to constitute a breach of unsecured PHI for which notification under the Breach Rule is required.

Procedure: Notification – If the Privacy Officer and/or designee determines that a breach has occurred, the Privacy Officer and/ or designee shall notify the patient or their personal representative without unreasonable delay and in no case later than 60 days of discovering the breach.

Notification

Patient Notification

1. After a complete investigation, no later than 60 days from breach discovery, the Privacy Officer and/or designee shall provide written notice to the patient or:
    a. If the patient is deceased, the next of kin or personal representative.
    b. If the patient is incapacitated/incompetent, the personal representative.
    c. If the patient is a minor, the parent or guardian.
2. Written notification must be in plain language with certain required information as described below.

3. Written notification must be sent to the last known address of the patient or next of kin, or if specified by the patient, by encrypted electronic mail. The template letter in this Breach Notification Policy will be used when sending written notification to a patient, personal representative, or next of kin.
4. In the case where there is insufficient or out-of-date contact information:
    a. For less than ten (10) individuals that precludes direct written notification to the patient, a substitute form of notice shall be provided such as a telephone call.
    b. In the case that there are ten (10) or more individuals for which there is insufficient or out of date contact information and contact information is not obtained, EMSA will:
        i. Post a conspicuous notice for 90 days on the homepage of their website that includes a toll-free number; or
        ii. Provide notice in major print or broadcast media in the geographic area where a patient can learn whether or not their unsecured PHI is possibly included in the breach. A toll-free number must be included in the notice. If EMSA utilizes major print or broadcast media, the Privacy Officer and/or designee will work with appropriate personnel to coordinate this activity.
5. If the Privacy Officer and/or designee determines the patient will be notified urgently of a breach because of possible imminent misuse of unsecured PHI, the Privacy Officer and/or designee will, in addition to providing notice as outlined above, contact the patient by telephone or other means, as appropriate.

Media Notification

1. In the case where a single breach event affected more than 500 residents of the same State or jurisdiction, notice shall be provided to prominent media outlets.
2. The Privacy Official and/or designee will work with appropriate support personnel to coordinate this notification.

HHS Notification

1. Notice will be provided by the Privacy Officer and/or designee without unreasonable delay and in no case later than 60 days from the breach discovery to the Secretary of the Department of Health and Human Services (HHS) if a single breach event was with respect to 500 or more individuals regardless of the State or jurisdiction. EMSA will use the template letter in this Breach Notification Policy when notifying HHS of breaches involving 500 or more individuals.
2. If a breach is with respect to less than 500 individuals, the Privacy Officer and/or designee will maintain a log of any such breach occurrence that occurred that year and annually submit the log to HHS no later than 60 days after the end of the calendar year. The template spreadsheet in this Breach Notification Policy will be used for reporting these annually to HHS, unless otherwise directed by HHS.

Content of Notification

Regardless of the method by which the notice is provided to patients, notice of the breach must include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured PHI that were involved in the breach;
3. The steps the individual should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what EMSA is doing to investigate the breach, mitigate harm to the individual, and to protect against any further breaches;
5. Contact information for follow-up questions (including a toll-free telephone number, an e-mail address, website, or postal address).

Administrative Procedures

The HIPAA Policies and Procedures for Employee HIPAA Training and HIPAA Disciplinary Procedure shall also apply with respect to these breach notification rule policies and procedures.

References

1. American Recovery and Reinvestment Act of 2009
2. Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164
3. HITECH Breach Notification Reporting Process