Breach Notification
HIPAA Policy: Privacy 03

Summary: Provide instructions for handling unauthorized disclosure of PHI

Affected Individuals: Employees in HIPAA covered entities

Purpose of Policy

To establish a process for handling breach notifications as they relate to breaches of unsecured PHI.

Scope

The University of Mississippi (UM) Breach of Unsecured Protected Health Information Notification Policy is established to facilitate institutional compliance with handling unsecured PHI breach notifications as required by the Health Insurance Portability and Accountability Act (HIPAA) and amended by Health Information Technology for Economic and Clinical Health (HITECH) Act.

Standards

In the event UM discovers a breach of Unsecured PHI, which demonstrates a probability that the PHI has been compromised based on a four factor risk assessment (greater than a low probability), it will be reported to the UM HIPAA Compliance Committee (HCC). The HCC will notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used or disclosed as a result of such breach. The HCC will also notify the Office of Integrity and Compliance at the University of Mississippi Medical Center.

The four factor risk assessment includes:

a. The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification;
b. The unauthorized person who used the PHI or to whom the disclosure was made;
c. Whether the PHI was actually acquired or viewed; and
d. The extent to which the risk of PHI has been mitigated.

The notification requirement applies to any Unsecured PHI accessed, maintained, retained, modified, recorded, stored, or otherwise held, used or disclosed by UM. The notification requirements also apply to breaches committed by UM or one of its Business Associates.

For purposes of this policy, a breach will be treated as discovered by UM or a Business Associate as of the first day on which the breach is known to UM or one of its Business Associates or by exercising reasonable diligence would have been known, respectively, including any person, other than the individual committing the breach, that is an employee, officer, or other agent of UM or a Business Associate.

Breach Notification
HIPAA Policy: Privacy 03

All individuals must immediately report any suspected PHI breach to the HCC. An individual can and will be subject to disciplinary actions for failing to report a known breach.

Definitions

The term "breach" means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

The term "breach" does not include:

a) any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the Company or Business Associate if-

   i. such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with UM or a Business Associate; and

   ii. such information is not further used or disclosed in a manner not allowed by HIPAA; or

b) any inadvertent disclosure from an individual who is otherwise authorized to access PHI at UM or Business Associate to another similarly situated individual at UM; and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by HIPAA; or

c) any unauthorized disclosure in which an unauthorized person to whom protected health information is disclosed would not reasonably have been able to retain the information.

The term unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the HIPAA, as amended.

Procedure

Deadline for Notice

Unless otherwise specified below, UM must provide notifications of a breach of Unsecured PHI as soon as practicable and in no case later than sixty (60) calendar days after the discovery of a breach.

Methods of Notice

Notice to Patients

Notice of a breach provided to an individual must meet the following requirements:

a) The notice must be written in plain language and delivered to the individual by first-class mail addressed to the individual (or if the individual is deceased the next of kin or personal representative of the individual) at the individual's (or next of kin's or personal representative's) last known address. In the alternative, if the individual has so specified, the notification may be delivered by electronic mail. The notification may be provided in one or more mailings as information becomes available.

b) In the case in which there is insufficient, or out-of-date contact information that precludes direct written (or, if specified by the individual, electronic) notification, a substitute form of notice reasonably designed to reach the individual shall be provided as follows: (i) in the case that there are ten (10) or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period of (90) ninety days on the home page of the Web site of UM or conspicuous notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free number where an individual can learn whether or not the individual's Unsecured PHI is possibly included in the breach; (ii) in the case of fewer than ten (10) individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means; (iii) if the individuals are deceased and there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual, then substitute notice is not required.

c) If UM determines that immediate notification is required because of possible imminent misuse of Unsecured PHI, UM may provide information by telephone or other means, as appropriate, in addition to the written notification required.

Notice to Media

Notice shall be provided to prominent media outlets of the relevant State or jurisdiction, following the discovery of a breach of Unsecured PHI, if the Unsecured PHI of more than 500 residents of a State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

Notice to HHS

Notice shall be provided to the Secretary of the Department of Health and Human Services (HHS) (Secretary) of unsecured PHI that has been acquired or disclosed in a breach. If a breach involved 500 or more individuals, such notice must be provided (i) without unreasonable delay; (ii) no later than sixty (60) days; and (iii) in the manner set forth on the HHS Office for Civil Rights website. If a breach involved less than 500 individuals, UM will maintain a log of any such breach discovered and annually submit the log to the Secretary in the manner set forth on the HHS Office for Civil Rights website documenting the breaches discovered during the year involved. This report will be made no later than

60 days after the end of the calendar year. The internal log (with supporting documentation) shall be maintained for six (6) years.

Content of Notification

Regardless of the method by which notice is provided to individuals as set forth above, notice of a breach shall be written in plain language and include, to the extent possible, the following:

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 PHI that were involved in the breach (such as full name, social security number, date of birth, home address, account number, diagnosis or disability code or other types of information).

c) The steps individuals should take to protect themselves from potential harm resulting from the breach.

d) A brief description of what UM is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches.

e) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Delay of Notification

Notification may be delayed if a law enforcement official determines that a notification, notice or posting would impede a criminal investigation or cause damage to national security.

Contact Information

For questions about the UM Breach Notification Policy or for more information, call the UM Office of General Counsel at 662-915-7014.