University of Wisconsin-Madison
Policy and Procedure

Policy Number: HIPAA 8.8
Policy Title: Reporting of HIPAA Incidents and Notifications in the Case of Breaches of Unsecured Protected Health Information
Effective Date: September 30, 2014
Last Revision Date: November 21, 2017

I. Policy

The Health Information Technology for Economic and Clinical Health Act regulations ("HITECH") amended the Health Information Portability and Accountability Act ("HIPAA") to establish requirements for notifying individuals in the event of a breach (as defined by HIPAA) of their unsecured Protected Health Information ("PHI"). In addition, HITECH contains requirements for notifying the Office of Civil Rights ("OCR") regarding breaches.

UW-Madison investigates potential breaches of PHI (referred to hereafter as "incidents") and determines if any incident meets HIPAA's definition of a breach, therefore requiring breach notification according to HITECH. UW-Madison makes notifications in the manner required by HITECH.

II. Definitions

A. **Discovery**: The first day on which an incident is known to UW-Madison (including by any person, other than the individual committing the breach, that is an employee, officer, or other agent of UW-Madison) or should reasonably have been known to UW-Madison to have occurred.

B. **Breach**: The acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI; any such acquisition, access, use, or disclosure is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.[1]

Breach excludes:

[1] 45 CFR § 164.402

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 that person's authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

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 under the HIPAA Privacy Rule.

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.

C. **Disclosure:** The release, transfer, provision of access to, or divulging in any manner of PHI by an individual within the UW HCC or UW ACE (see definitions below) with a person or entity outside the UW HCC or UW ACE.

D. **Protected Health Information ("PHI")**: Individually identifiable health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. PHI does not include student records held by educational institutions or employment records held by employers.[2]

E. **University of Wisconsin Affiliated Covered Entity ("UW ACE")**: The UW-Madison Health Care Component (except University Health Services and the State Laboratory of Hygiene), the University of Wisconsin Medical Foundation and the University of Wisconsin Hospital and Clinics. See HIPAA Policy # 1.2 "Designation of UW Affiliated Covered Entity."

[2] See 45 CFR § 164.503 for complete definition and exclusions.

F. **University of Wisconsin-Madison Health Care Component ("UW HCC")**: Those units of the University of Wisconsin-Madison that have been designated by the University as part of its health care component under HIPAA. See Privacy Policy # 1.1 "Designation of UW-Madison Health Care Component" for a listing of these units.

G. **Unsecured PHI**: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Department of Health and Human Services.

III. Procedures

A. Investigations of Incidents (Paper or Oral Only)

1. Anyone who becomes aware of an incident involving paper records or oral statements only must report the incident to the UW-Madison HIPAA Privacy Officer within 24 hours of the discovery of the incident.

   HIPAA incident reports should be submitted online via the reporting mechanism available at compliance.wisc.edu/hipaa.

2. Examples of incidents involving paper records or oral statements only include:

   - A patient is handed a copy of the wrong After Visit Summary;
   - A health care provider is overheard discussing a patient's identifiable medical information in the elevator or cafeteria.
   - An abstract or poster for a presentation at an event or conference contains PHI and does not reference obtaining appropriate authorization.
   - Postcards are mailed to patients or research subjects which name diagnoses or specific therapies in addition to full names and addresses.

3. To the extent applicable, the HIPAA Privacy Officer will notify the HIPAA Privacy Coordinator of the applicable UW HCC unit within 24 hours of being notified of an incident.

4. The HIPAA Privacy Officer shall lead the investigation and, in coordination with the HIPAA Privacy Coordinator of the applicable UW HCC unit or his/her designee, shall complete the UW-Madison HIPAA Breach Analysis Form as soon as practicably possible, absent exigent circumstances. The HIPAA Privacy Officer shall notify the HIPAA Privacy and Security Operations Committee of the investigation and, if an investigation appears likely to continue beyond 14 calendar days, shall also provide the reason for the delay.

5. The HIPAA Privacy Officer shall maintain a log of all reported incidents along with information from the HIPAA Breach Analysis Form and information about any notices sent to affected individuals, media outlets, and the Office of Civil Rights of the Department of Health and Human Services ("OCR").

B. All Other Investigations of Incidents

1. Anyone who becomes aware of an incident other than those described in III.A. above must report the incident to the HIPAA Privacy Officer or the HIPAA Security Officer within 24 hours of the discovery of the incident. The HIPAA Privacy Officer an dHIPAA Security Officer shall collaborate with local/department IT staff to determine how best to initiate an investigation about an incident.

   HIPAA incident reports should be submitted online via the reporting mechanism available at compliance.wisc.edu/hipaa.

2. If an incident is reported to a local/department IT office, that office shall immediately notify the HIPAA Privacy Officer or HIPAA Security Officer, and also submit the details of the incident online via the reporting mechanism available at compliance.wisc.edu/hipaa. The investigation shall then proceed as outlined in III.A.3-5, above.

3. If additional information from the UW-Madison Chief Information Officer ("CIO") is needed to investigate an incident, or as otherwise directed by the HIPAA Security Officer, the CIO's Chief Information Security Officer

("CISO") shall participate in the investigation and provide findings to the HIPAA Privacy and Security Officers without unreasonable delay and in no case more than 30 days from the date of discovery of the incident. The investigation shall then proceed as outlined in III.A.3-5, above.

4. If the HIPAA Security Officer or CIO determines that an Administrative Leadership Team ("ALT") should assemble as described in the CIO's Information Incident Reporting and Response Policy, the ALT shall include the HIPAA Privacy Officer. Upon completion of ALT's analysis, the investigation shall then proceed as outlined in III.A.3-5, above.

C. Breach Determination

1. The HIPAA Privacy Officer, in consultation with the UW-Madison HIPAA Security Officer and the HIPAA Privacy and Security Operations Committee, as needed or as time permits, will make the final determination of whether a breach has occurred.

2. The HIPAA Privacy Officer will notify the UW-Madison HIPAA Privacy and Security Executive Board of any required breach notifications.

D. Breach Notifications. If it is determined that a breach of unsecured PHI has occurred, the following notifications are made in accordance with HITECH regulations:

1. Notification to Affected Individuals.

a. Without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, the HIPAA Privacy Officer notifies each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of a breach.

b. The HIPAA Privacy Officer shall draft and sign any notification letter(s), in consultation as needed with the Privacy Coordinator

of the relevant HCC unit in the drafting. The UW-Madison Office of Compliance shall ensure timely mailing of any notification letter(s).

c. The notification, written in plain language, shall include, to the extent possible:

i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

ii. A description of the types of unsecured PHI that were involved in the breach (e.g., full name, social security number, date of birth, home address, account number, diagnosis, disability code, and/or other types of information);

iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

iv. A brief description of what UW-Madison is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

v. 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.

d. The notification required shall be provided in the following form:

i. 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 may be provided in one or more mailings as information is available.

ii. If UW-Madison knows 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 either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

e. If there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided (this does not apply to the next of kin or personal representative of the individual).

i. If there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

ii. If there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(a) Be in the form of either a conspicuous posting for a period of 90 days on the hippa.wisc.edu home page of, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(b) 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.

f. In any case deemed to require urgency because of possible imminent misuse of unsecured PHI, the HIPAA Privacy Officer

may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided as described above.

2. Notification to the Secretary of US Department of Health and Human Services (HHS).

   a. For a breach involving 500 or more individuals, the HIPAA Privacy Officer provides notification to the Secretary contemporaneously with the notice to affected individuals in the manner specified on the HHS Web site.

   b. For a breach involving less than 500 individuals, the HIPAA Privacy Officer or the Privacy and Security Program Coordinator at his/her direction, maintains a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provides the notification for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

3. Notification to the Media. For a breach involving more than 500 residents of the State, the UW-Madison HIPAA Privacy Officer in conjunction with University Communications shall, contemporaneously with the notice to affected individuals and to the Secretary of HHS, notify prominent media outlets serving the State.

4. Law Enforcement Delay. If a law enforcement official states that a notification, notice, or posting required by HIPAA would impede a criminal investigation or cause damage to national security, the HIPAA Privacy Officer shall:

   a. 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

   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.

5. The HIPAA Privacy Officer will notify the HIPAA Privacy and Security Operations Committee and the HIPAA Executive Board when all required notifications have been made.

E. In the event an incident involves research subjects, the HIPAA Privacy Officer shall notify the appropriate Intuitional Review Board ("IRB") upon learning of the incident if it is unclear that the IRB is already aware, and shall work with such IRB to ensure that any proposed remediation does not conflict with IRB determinations, policies or laws governing human subjects research.

F. Both breaches and incidents determined not to be breaches will be reported to the HIPAA Privacy and Security Operations Committee by the HIPAA Privacy Officer for discussion of possible remedial or preventive actions.

IV. Documentation Requirements

The UW-Madison HIPAA Breach Analysis Form must be completed for each incident investigation.

V. References

45 CFR Subpart D

VI. Related Policies

None

VII. For Further Information

For further information about this policy, please contact the UW-Madison HIPAA Privacy Officer. Contact information is available at compliance.wisc.edu/hipaa.

Reviewed By
UW-Madison HIPAA Privacy Officer
UW-Madison Office of Legal Affairs

Approved By
UW-Madison HIPAA Privacy and Security Operations Committee