


Emma Eccles Jones College of Education & Human Services

POLICY INFORMATION

Document # 202	Title: Breach Notification	Print Date: 8/08/2016
Revision # 1.0	Prepared by: J. Black	Date Prepared: 1/15/2016
Safeguard: HIPAA	Approved by: Dean Beth E. Foley 	Date Approved: 8/29/2016

I. POLICY STATEMENT

HIPAA establishes provisions for protecting the privacy and security of patient Protected Health Information (PHI). HIPAA requires that covered entities and their business associates provide notification following a breach of unsecured PHI. All CEHS HCC's will make appropriate disclosures following a breach of unsecured PHI.

II. DEFINITIONS

See HIPAA Privacy Policy 100

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the Health Care Component/HCC (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

IV. PROCEDURES TO IMPLEMENT

1. Identifying a Breach

An impermissible use or disclosure of PHI is presumed to be a breach unless CEHS or the business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on the Data Breach Investigation Guidelines (See Attachment A). The term "Breach" excludes:

- A. 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 authority and does not result in further use or disclosure in a manner not permitted by HIPAA;
- B. Any inadvertent disclosure by a person who is authorized to access PHI at a CEHS HCC or business associate to another person authorized to access PHI at the same HCC or business associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA;

Emma Eccles Jones College of Education & Human Services

- C. A disclosure of PHI where a HCC or BA 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; and
- D. A use or disclosure of a Limited Data Set, as long as the Limited Data Set excludes their date of birth and zip code.

The date of the breach is considered to be the date it is “discovered” by an HCC as of the first day on which such breach is known to the HCC, or, by exercising reasonable diligence would have been known to the HCC.

2. Internal Notification and Communication

- A. The HCC Privacy Officer and the CEHS Privacy and Security Officer(s) shall be notified of all potential unlawful or unauthorized access to, use of, or disclosure of potentially identifiable patient medical information as soon as detected.
- B. In the event that a Business Associate suffers a Breach, the Breach date would be the date that the BA notifies CEHS of the Breach.
- C. The Incident Response Team (IRT) will conduct an investigation and assessment. The Incident Response Team consists of, at a minimum:
 - a. The CEHS Privacy Officer
 - b. The CEHS Security Officer
 - c. USU Information Security Officer

3. Investigation and Performance of Risk Assessment

- A. The IRT will investigate and perform a risk assessment to determine whether a Breach has occurred and if so, whether notification to the affected individual(s) is required. (Refer to **Breach Investigation Guidelines - Attachment A.**)
- B. The IRT shall take immediate steps to mitigate harm. Mitigation steps may include, but are not limited to:
 - a. The return or retrieval of lost data;
 - b. Determining who used the PHI and whether the PHI was re-disclosed; and
 - c. Obtaining satisfactory assurances from a recipient of breached PHI that the information will be further used or disclosed, or that the PHI will be or has been destroyed.
- C. The IRT will gather documentation, conduct interviews, and perform other actions as needed to obtain evidence and will work together as a team to create an assessment of the results of the investigation.
- D. When a PHI Breach occurs at a BA, in addition to other requirements, the IRT and potentially USU legal department will discuss mitigation efforts, potential reimbursement by BA for costs and expenses related to the BA’s Breach, and whether changes in the BAA and BA relationship are required.
- E. Based on the IRT’s assessment, one of the following determinations will be made:
 - a. **Breach unfounded** - No violation has occurred.
 - b. **HIPAA Breach of more than 500 Individuals** - Breach has occurred and falls under the Breach notification requirements. Notification to the affected individuals, the media and HHS is required within 60 calendar

Emma Eccles Jones College of Education & Human Services

days after discovery of the Breach. USU legal and Public Relations departments are responsible for overseeing and approving all notification letters.

- c. **HIPAA Breach of less than 500 Individuals** - Breach has occurred and falls under the Breach notification requirements. The Privacy Officer shall keep a log of breaches of PHI and complete HHS's online form or other applicable procedures for each individual breach no later than 60 days after the end of each calendar year. Notifications must be made to the affected individuals (via USU legal and Public Relations departments) and a log must be kept by the HCC.

4. Breach Notification

A. Patient Notifications

- a. Letters to Individuals - Without unreasonable delay and in no case later than 60 calendar days after the discovery, the HCC Privacy Officer shall mail the approved patient Breach notification letter via first-class mail to all impacted patients or patient representatives. The HCC Privacy Officer is responsible to identify and gather all affected individual's information. The notification letter should contain all of the required elements and be approved by USU Legal Department. A copy of the letter and all associated materials must be maintained by the Privacy Officer for a minimum of six years. An Accounting of Disclosures must be maintained by CEHS when a breach has been determined to have occurred.
- b. Insufficient Contact Information: Substitute Notice to Fewer than Ten Individuals - If there is insufficient or out-of-date information that prevents direct written communication with the patient, a substitute form of notice (e.g., telephone call) shall be utilized if fewer than ten patients are involved.
- c. Insufficient Contact Information: Substitute Notice to more than ten individuals - If there are ten or more patients involved, a conspicuous posting for 90 days can be posted on the HCC and/or CEHS website or notice in major print or broadcast media where the patients affected by the Breach are likely to reside.
- d. Media Notification: Breach of 500+ Individuals - In the case of a single Breach event involving 500 or more patients in the same State, notice must be provided to prominent media outlets serving in the area. Such notice must be provided without unreasonable delay and in no case later than sixty days after discovery of the breach. The media notice must contain the same informational elements that are in the letter to individuals. Media Notification will be handled by USU's Public Relations Department.
- e. HHS Notification - The HHS requires that entities report Breaches. A report of a Breach to HHS may only be made by the CEHS Privacy and/or

Emma Eccles Jones College of Education & Human Services

Security Officer, USU Information Security Officer or USU Legal
Department.

V. ATTACHMENTS

Attachment A - Breach Investigation Guidelines

VI. REFERENCES

45 CFR §164.530(f)

45 CFR §164.404

45 CFR §164.404(d)(2)(i)

45 CFR §164.406

45 CFR §164.408

Emma Eccles Jones College of Education & Human Services

**Attachment A
Data Breach Investigation Guidelines**

The members of the Incident Response Team (IRT) should consider:

- A. Is this incident a violation of the HIPAA Privacy Rule?
 - a. Was the information PHI?
 - b. Did the use or disclosure of PHI fall within an exception to the definition of “Breach?”
 - c. Was the use or disclosure of PHI impermissible under the HIPAA privacy regulations?
 - d. If the information was not PHI, does the information trigger other federal or state breach laws?
- B. Does the violation compromise the security or privacy of the PHI?
- C. What type(s) and amount of PHI and other information were lost?
 - a. *Examples:* Dates of Birth, Social Security Numbers, names, address, diagnosis, diagnostic codes, account numbers, dates of admission, email addresses, etc.
- D. Does the violation pose a significant risk of financial, reputational, or other harm to the individual?
 - a. Will the information embarrass the individual or damage his/her reputation?
 - b. What is the likelihood the individual could suffer economic harm, such as identity theft (whether it be medical or other)?
- E. Who used the information and was it re-disclosed, and if so, to whom?
- F. What mitigation successful in significantly reducing or eliminating the risk of harm to the individual?
 - a. If mitigation efforts eliminate or reduce the risk of harm to the individual to less than a “significant risk” of financial, reputational or other harm, then the privacy of the PHI was not compromised and no breach has occurred.