TITLE

Breach of Protected Health Information

PURPOSE

In accordance with 45 CFR Subpart D, this procedure provides guidance to The University of Arizona (UA) Health Care Components (HCCs) regarding the discovery, notification and remediation of breaches of Protected Health Information (PHI) and Electronic Protected Health Information (e-PHI). In accordance with 45 CFR Subpart D, this procedure provides guidance to The University of Arizona (UA) Health Care Components (HCCs) regarding the discovery, notification and remediation of breaches of PHI and e-PHI.

REVIEW/REVISIONS

- 06/2015

REFERENCES AND RELATED FORMS

- Capitalized terms are defined in HIPAA Privacy Program Guidance (Definitions of Key Words) and 45 CFR Parts 160 and 164
- HIPAA Privacy Program Procedure 140 (Complaints and Investigations)

PROCEDURES

1. Background: Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA and which compromises the security or privacy of the protected health information.
    A. Exclusions:
        i. 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 under HIPAA.
        ii. 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 HIPAA.
        iii. 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.
    B. Risk Assessment: An impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as

applicable, demonstrates that there is a low probability that PHI has been compromised based on a risk assessment of at least the following factors:

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

2. Breach: HCCs will implement procedures and practices to protect against breaches of PHI.
   A. In the event of a breach of PHI, HCCs must:
      i. Immediately notify the HIPAA Privacy Program;
      ii. Cooperate with the HIPAA Privacy Program, Information Security Office and others in the course of the investigation of the breach; and
      iii. In coordination with the HIPAA Privacy Program, initiate corrective action plans or other remediation or mitigation to prevent recurrence of the breach or similar breaches.
   B. When applicable, the Privacy and Security Breach Team (see below) will implement the breach protocol (Protocol), which outlines the necessary steps to take in the event that any confidential or restricted data is compromised.
      i. This Protocol includes assembling key UA stakeholders and is also used to perform the risk assessment as identified under 45 CFR § 164.402.
      ii. Unless the PHI in question is indecipherable, unreadable, or unusable, the HIPAA Privacy Program will determine through a risk assessment whether the incident meets the definition of breach under 45 CFR § 164.402.
      iii. The HIPAA Breach Team shall consist of, at a minimum:
         1. HIPAA Privacy Officer and/or his/her designees;
         2. Information Security Officer and/or his/her designees;
         3. Representative(s) from the UA Office of General Counsel (OGC); and
         4. Any other individuals identified as necessary participants.
   C. Reporting:
      i. To OCR: When necessary, the HIPAA Privacy Program will report breaches involving HCCs to the Secretary of the Department of Health and Human Services and coordinate any or all investigations the Secretary may perform or cause to be performed.
         1. The Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information can be found here: https://ocrnotifications.hhs.gov/
      ii. To Others: The HIPAA Privacy Program will work with the Information Security Office or designated UA point-of-contact for breach notifications

to notify the Office of University Communications to coordinate notification to individuals and notification to the media, as necessary.

3. Breaches affecting less than 500 individuals:
   A. Breach information must be added to the breach log by the HIPAA Privacy Program;
   B. The HIPAA Privacy Program will work with the Information Security Office or designated UA point-of-contact for breach notifications to affected individuals within sixty (60) calendar days after discovery of a breach; and
   C. The HIPAA Privacy Program must submit the breach log to OCR no later than February 1 of each calendar year.

4. Breaches affecting more than 500 individuals:
   A. Breach information must be added to the breach log by the HIPAA Privacy Program;
   B. The HIPAA Privacy Program will work with the Information Security Office or designated UA point-of-contact for breach notifications to affected individuals;
   C. The HIPAA Privacy Program will work with the Information Security Office or designated UA point-of-contact for breach notifications to notify the Office of University Communications to coordinate notification to the media; and
   D. Notice shall be provided to the Secretary of HHS by the HIPAA Privacy Program without unreasonable delay and in no case later than sixty (60) calendar days in the case of a single Breach event involving 500 or more individuals, regardless of the location of the patients.

5. Role of the HIPAA Privacy Program: The HIPAA Privacy Program will work with the HCC and the Information Security Office to investigate the circumstances of the breach and make recommendations regarding a corrective action plan or other remediation.[1]

6. Role of Information Security Office: The Information Security Office collaborates with the HCC and with the HIPAA Privacy Program to investigate the circumstances of the breach and make recommendations regarding a corrective action plan or other remediation.

   The Information Security Office may recommend appropriate remediation action, provide additional training to staff and recommend other process improvements as necessary to remediate the breach and prevent recurrences.

   Please see UA Information Security guidance (including, but not limited to, IS-100, IS-S1100, IS-P1100, IS-G1100) for incident and breach response guidelines.

[1] See HIPAA Privacy Program Procedure 500 for compliant procedures.

7. Documentation: The HIPAA Privacy Program will maintain complete and accurate documentation of reported/suspected breaches, investigations, remedial action and all other activities associated with the breach for at least six years.