PROTECTED HEALTH INFORMATION DATA BREACH NOTIFICATION RULE

I. Purpose

A. This rule provides guidance and direction with regard to notifying patients and/or research participants in the event of a breach of protected health information. This rule does not change the University's responsibilities with respect to the Health Insurance Portability and Accountability Act's ("HIPAA") Privacy and Information Security regulations and safeguarding protected health information.

II. Scope

A. This rule is applicable to all protected health information within the University of Utah regardless of its use (academics, administrative/operational, clinical, research, etc).

III. Definitions

A. Breach means the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information.

B. Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached.

C. Protected Health Information ("PHI") means any information, whether oral or recorded in any form or medium that meets **both** of the following criteria:

1. It is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse.
2. It relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

D. Redaction means marking or blacking out of the protected health information in a document.

E. Secured means protected health information that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals as specified in the guidance attached to this rule.

F. Unauthorized means any use or disclosure that would violate the HIPAA Privacy and Security Rules.

IV. Rule

A. Breaches: All breaches of protected health information must be reported as soon as possible, but no later than 24 hours after the breach is identified.

1. Breaches will be reported to the Health Sciences Service Desk at 801-587-6000 or the University Service Desk at 801-581-4000.
2. The Service Desk(s) will report the incident immediately to the Information Security and Privacy Office.
3. The Information Security and Privacy Office will conduct a risk assessment of the reported incident to confirm that the incident meets the definition of a "breach".

a. If a breach is confirmed, it is deemed to be "discovered" and the timing for notification begins to toll immediately[1].
b. Notification will be made without unreasonable delay and no later than 60 days after being discovered.
c. If a law enforcement official determines that a notification, notice, or posting required by this rule would impede a criminal investigation or cause damage to national security, and notifies the Information Security and Privacy Office, such notification, notice, or posting shall be delayed.[2]

4. Once a breach is substantiated, Breach Notification Procedures will be initiated by the Information Security and Privacy Office.
5. The department responsible for the confirmed breach will be accountable for all costs associated with notification and for accomplishing all tasks required by Breach Notification Procedures. The department may also have to complete a corrective action plan to help reduce the risk of a future breach.

B. The following technologies and methods shall be used to render PHI secured for purposes of this data breach notification rule. Guidance addressing technology and methods is attached to this rule.
1. Encryption. The use of a National Institutes of Standards and Technology ("NIST") approved algorithm and procedure is preferred and may allow for "safe harbor."
2. Destruction: paper, film, or other hard copy must be shredded or destroyed at end-of-life or use such that the PHI cannot be read or otherwise reconstructed and is rendered unusable, unreadable, or indecipherable.
3. Electronic media containing PHI must be cleared, purged, or destroyed consistent with approved NIST guidelines for media sanitization such that the PHI cannot be retrieved[3].
4. Redaction of paper records is *not* an approved method of rendering PHI unusable, unreadable, or indecipherable.

C. The Information Security and Privacy Office will provide training to workforce members on:
1. strategies for discovering and reporting suspected or actual breaches to the Information Security and Privacy Office;
2. the importance of reporting; and
3. consequences and sanctions of failure to report.

D. Reporting breaches is mandatory. Violation of this rule may result in disciplinary action in accordance with University policies referenced in Section VI of this rule[4].

E. University of Utah staff, faculty, students, or other individuals are prohibited from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for by this rule[5].

V. Procedures, Guidelines, Forms and other related resources

---

[1] In response to the RFI, some commenters suggested that suspected but unconfirmed breaches should not be treated as discovered until all the facts of the breach could be confirmed. Others suggested that 60 days was an insufficient amount of time to conduct a complete investigation and send the required notifications. We disagree.
[2] 13402(g)
[3] Breach Notification Rules, supra note 3 at page 42743
[4] 164.530(e)
[5] 164.530(g)

A. Procedures
    1. Information Security and Privacy Incident Response Procedures
B. Guidelines
    1. Memo: Technology and methods used to render protected health information secured
    2. Memo: Examples of data breaches that must be reported under HI Tech
    3. NIST and FIPS Standards: http://www.csrc.nist.gov/

VI. References
A. Policy 4-001: Institutional Data Management Policy
B. Policy 4-004: University Information Technology Resource Security Policy
C. Policy 5-111, Disciplinary Actions and Dismissal of Staff Employees
D. Policy 6-400, Code of Student Rights and Responsibilities
E. Policy 6-316, Code of Faculty Rights and Responsibilities
F. Health Insurance Portability and Accountability Act of 1996, "HIPAA" (PL 104-191)
G. HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164)
H. American Recovery and Reinvestment Act (PL 111-5), Title XIII – Health Information Technology, Section 13402

VII. Contacts:
A. Policy Officer: Chief Information Officer, 801-581-3100
B. Policy Owner: Chief Information Security and Privacy Officer, 801-587-9241
C. compliance@utah.edu

VIII. History: