

UNIVERSITY OF OKLAHOMA

HIPAA Privacy Policies

Subject: Breach of Unsecured PHI	Coverage: Health Care Components
Policy: Privacy 34	Page: 1 of 3
HITECH Act Section: 13402	Approved:
Effective Date: 9/22/2009	Revised:

I. PURPOSE

To provide for notification in the case of breaches of unsecured protected health information. For purposes of these requirements, section 13402(h) of the HITECH Act (“Act”) defines “unsecured protected health information” to mean protected health information that is not secured through the use of approved technologies or methodologies.

To be approved, technologies and methodologies must render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

II. POLICY

The University, through its Health Care Components, will implement reasonable and appropriate technologies and methodologies designed to secure protected health information from unauthorized disclosure.

If PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals, then the PHI is not “unsecured” PHI.

This policy establishes the requirements as outlined by the Act regarding the protection of PHI that each Health Care Component must comply with and the notification that must occur in the event of a breach. The breach notification provisions of section 13402 of the Act apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI.

Each Health Care Component shall designate an individual to be responsible for compliance with this policy, in coordination with the HIPAA Privacy and Security Officials.

1. Methods of Protection – Either of the following methods may be used to secure PHI and make it unusable, unreadable, or indecipherable to unauthorized individuals.
 - a. **Encryption** – The University and each Health Care Component will implement and maintain reasonable and appropriate encryption technologies and methodologies to enhance the protection of PHI.
 - i. Refer to University Security policies (available on the Information Technology webpage) for encryption requirements.
 - b. **Destruction** – The University and each Health Care Component will implement destruction techniques that render PHI unusable and/or unreadable in any format.
 - i. Refer to University Security policies (available on the Information Technology webpage) for destruction requirements.

PHI secured by one of the above methods is not insecure and is therefore not subject to this policy.

For additional information on the guidelines and standards of encryption and destruction methods, contact Information Technology or visit <http://it.ouhsc.edu/policies>.

2. Notification of Breach
 - a. In the event a breach of unsecured PHI is discovered, the University or its designee is required to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed, according to the requirements of the Act:
 - i. Written notice to the individual (or next of kin if the individual is deceased) at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if specified by the individual);
 - ii. In the case in which there is insufficient or out-of-date contact information, substitute notice, including, in the case of 10 or more individuals for which there is insufficient contact information, conspicuous posting (for a period determined by the Secretary) on the home page of the web site of the University or notice in major print or broadcast media;
 - iii. In cases that the Health Care Component or University deem urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the above methods.
 - b. Details of the notice shall include the following:
 - 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

(such as full name, SSN, DOB, home address, account number, or disability code);

- iii. The steps individuals should take to protect themselves from potential harm resulting from the breach;
 - iv. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
 - 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.
- c. If a breach involves more than 500 individuals, the HIPAA Privacy and Security Officials must be notified immediately. They will determine whether and when a notice to the individual, the media, and/or HHS is appropriate and, if so, the content of the notice.

3. Tracking

- a. Health care components must maintain a log of breaches of unsecure PHI and notify the HIPAA Privacy Official of each breach.
- b. The University, through the HIPAA Privacy Official, shall maintain a log of all reported breaches of unsecure PHI and shall submit required reports of such to the Secretary of HHS annually, as required by the Act.

III. REFERENCES

1. HITECH Act Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009, (effective February 17, 2009)
2. HITECH Act Breach Notification Regulations (effective September 2009)
3. Department of Health and Human Services
4. HIPAA Privacy & Security Rules 45 CFR Parts 160, 162, and 164
5. NIST SP 800-111 "*Guide to Storage Encryption Technologies for End User Devices*" and SP 800-88 "*Guidelines for Media Sanitization*"
6. Oklahoma State Breach Notification Law, Section 298 [HB 2357], (effective June 8, 2006)
7. Oklahoma State Breach Notification Law, [HB 2245], (effective November. 1, 2008)