Oklahoma State University

Title: Definitions	**Policy #: BRE-01.00**
Category: HIPAA Compliance	**Authority: 45 CFR § HIPAA SECTION: 164.402**
Standard: Notification in the Case of Breach of Unsecured Protected Health Information	**Responsibility: Health Care Components**
Effective Date: 09-23-2009	**Page 1 of 3**
Approved By: OSU Legal Counsel	**Revised: 06-01-2013**

PURPOSE:
To define various words used in this section of policies and procedures applicable to Breach Notification.

POLICY:

As used in this section, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information 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 The Privacy Rule.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information 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 Privacy Rule.

(iii) A disclosure of protected health information 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.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low

probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

Oklahoma State Law definitions: *os_74-3113.1 Breach*

1. Breach of the security of the system means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the state agency, board, commission or other unit or subdivision of state government. Good faith acquisition of personal information by an employee or agent of the state agency, board, commission or other unit or subdivision of state government for the purposes of that entity shall not be a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure;

2. *Personal information* means the first name or first initial and last name of an individual in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

a. social security number,
b. driver license number, or
c. account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the financial account of an individual.

Personal information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local public records; and

3. *Notice* means one of the following methods:

a. written notice,
b. electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code, and
c. substitute notice, if the agency demonstrates that the cost of providing notice would exceed Two Hundred Fifty Thousand Dollars ($250,000.00), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
   (1) e-mail notice when the agency has an e-mail address for the subject persons,
   (2) conspicuous posting of the notice on the agency's web site page, if the agency maintains one, and
   (3) notification to major statewide media.