Oklahoma State University

Title: Response and Reporting	**Policy #: SEC-05.01**
Category: HIPAA Compliance	**Authority: 45 CFR § HIPAA SECTION: 164.308(a)(6)(ii)**
Standard: Security Incident Procedures	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Pages: Page 1 of 2**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

PURPOSE:

Security Incident Procedures for Response and Reporting

POLICY:

OSU will identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to OSU; and document security incidents and their outcomes. *§164.308(a)(6)(ii)*

PROCEDURE:

OSU will designate an individual who will be responsible for implementing and adhering to the security incident policies and procedures.

OSU will determine through a variety of security mechanisms, such as User-ID'S, password protection, anti-virus software and audit trails when security incidents have occurred.

Security incidents must be reported by personnel who observe questionable activity. Personnel identified security incidents are reported to the person's direct supervisor or higher level or management who in turn reports the incident to the HIPAA Compliance Office.

OSU will periodically monitor user activity, including password activity, virus scans, and audit trails to determine if any security incidents have occurred.

Following the identification of a security incident, the first priority must be to communicate the details of the incident to the IT and HIT Directors and/or technical systems manager to expeditiously log and begin resolving the issue. Also, the OSU Medical Director and the CFS Director should be notified of the incident.

Once alerted to the incident, the technical staff or designee(s) will access the appropriate part of the computer system as quickly as possible. If more than one incident occurs simultaneously, the most critical issue will be addressed first. If necessary, OSU Stillwater Security Staff may be utilized to conduct computer forensics and analysis. In some instances, OSU legal counsel may be involved.

Oklahoma State University

Title: Response and Reporting	**Policy #: SEC-05.01**
Category: HIPAA Compliance	**Authority: 45 CFR § HIPAA SECTION: 164.308(a)(6)(ii)**
Standard: Security Incident Procedures	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Pages: Page 2 of 2**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

The incident(s) will be immediately logged on a security incident log. OSU will take necessary and reasonable steps to respond to and address all identified and confirmed security incidents. All responses will be logged into a security incident log. The log will be kept for 6 years.

If the incident cannot be resolved and could potentially cause disruptions among other OSU employees such that it will inhibit them from performing their assigned job responsibilities, the appropriate director will notify the staff of the situation via the appropriate communications media (ie. email, telephone, verbally, or in writing). Affected staff will be notified of the estimated time necessary to address the security incident.

Once the issue has been resolved, the System Administrator or Security Official will notify OSU staff of the resolution via email, telephone, verbally, or in writing. If there are new procedures which must take place a result of the reported incident, these must be distributed to OSU employees as well. The practice should select the communication media that works best under the circumstances.

Example of Security Incident Log

Incident	Time and Date Incident Reported	Time and Date Incident Occurred	Incident Reported By	Incident Handled By	Practice Individuals Notified	Responses