

CLIN 207 - HIPAA SECURITY RISK ANALYSIS AND MANAGEMENT

Policy

1. In accordance with the HIPAA Security Rule¹, USC² maintains a HIPAA security risk analysis and management program to assess and prioritize risks to the confidentiality, integrity and availability of Protected Health Information (PHI)³ and to respond, accept or remediate as appropriate. USC's risk analysis and management program shall be aligned to USC's strategic plan, goals and priorities.
2. The risk analysis shall take into account all types of PHI, regardless of the particular medium in which it is created, received, maintained or transmitted or the source or location.
3. The security risk analysis shall evaluate the following to determine the risk level:
 - a. **Criticality of Information/Asset.** The operational and financial impact if the information/asset was lost, breached or the operations were disrupted;
 - b. **Threats/Vulnerabilities to the Information/Asset.** Technical/cyber, physical, environmental and human threats/vulnerabilities to the information/asset;
 - c. **The potential impact** of the threat/vulnerability;
 - d. **The likelihood of occurrence** of the threat/vulnerability; and
 - e. **Mitigating controls.**
4. Threat impact, likelihood and mitigating controls should be rated based on an appropriate criteria rating, such as the criteria rating used for the university's enterprise risk

¹ 45 C.F.R. 164.308

² For purposes of HIPAA, USC includes: Those entities that comprise Keck Medicine of USC (USC Norris Cancer Hospital, Keck Hospital of USC, the Keck Doctors of USC, USC Care Medical Group, affiliated medical foundations of Keck and their physicians, nurses and clinical personnel, USC Verdugo Hills Hospital, its nurses and other clinical personnel, Verdugo Radiology Medical Group, Verdugo Hills Anesthesia, and Chandnish K. Ahluwalia, M.D., Inc.); USC's employed physicians, nurses and other clinical personnel; those units of USC that provide clinical services within the Keck School of Medicine, School of Pharmacy, the Herman Ostrow School of Dentistry (including Physical and Occupational Therapy); and those units that support clinical and clinical research functions, including the Offices of the General Counsel, Audit and Compliance.

³ Protected Health Information is defined as identifiable information that relates to the individual's past, present or future physical or mental health condition or to payment for health care. ePHI is PHI that is transmitted by electronic media or is maintained in electronic media. For example, ePHI includes all data that may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

| | | |
|--------------|--|---|
| Issued by: | Michael Quick Provost and Senior Vice President, Academic Affairs | Todd R. Dickey Senior Vice President, Administration |
| Date issued: | March 1, 2016 University of Southern California Page 1 of 3 | |

assessment process. The ratings criteria may be modified as necessary to accurately reflect the applicable risk levels.

5. The HIPAA security risk analysis results will be the basis for development of the HIPAA security risk management plan. It also shall be evaluated and incorporated, as appropriate, into the university-wide enterprise risk assessment process.
6. The HIPAA security risk analysis and management plan will be reported to the Information Risk Committee and senior management, as appropriate.
7. The risk analysis process is ongoing and should be re-evaluated as needed, and at least annually, to review existing systems/assets and to incorporate material new purchases, projects, data downloads, security incidents or other major changes to systems/assets, processes or personnel.

Procedure

1. The following information and processes should be considered in assessing, analyzing and prioritizing USC's risks in protecting and securing health information:
 - A. **ePHI Inventory**: Those clinical units with ePHI will develop and maintain a process for reviewing and updating an ePHI inventory, which includes e-PHI that the unit creates, receives, maintains or transmits. e-PHI can be identified using various data gathering techniques, including a review of past or current projects, interviews, and data discovery tools, such as data loss prevention (DLP) tools. The clinical units will provide the ePHI inventory to the Information Security office and the Office of Compliance, upon request.
 - B. **HIPAA System Risk Assessments**: Clinical units should complete a HIPAA risk assessment on each system identified on the clinical unit's ePHI inventory (see Exhibit A). The HIPAA Risk Assessment will assist in evaluating the criticality of the system/asset and the potential and actual threats and vulnerabilities.
 - C. **Vulnerability Scans**: Clinical units should incorporate the results of their respective vulnerability scans into their system risk assessments to assist in evaluating the severity and likelihood of actual and potential vulnerabilities.
 - D. **PHI Data management**: Clinical units should track and monitor internal uses of PHI, such as through network and PHI data flow diagrams, as appropriate, to confirm minimum necessary standards and appropriate security measures are maintained. Third-party party vendors and suppliers that create, receive, maintain or transmit e-PHI should execute USC's template Business Associate Agreement. Clinical units

| | | |
|--------------|--|---|
| Issued by: | Michael Quick Provost and Senior Vice President, Academic Affairs | Todd R. Dickey Senior Vice President, Administration |
| Date issued: | March 1, 2016 University of Southern California Page 2 of 3 | |

should conduct appropriate due diligence to confirm that the vendor can meet the obligations contained in the Business Associate Agreement.

2. The risk analysis also should consider findings and recommendations from USC internal and external audits as well as national and global trends, issues or other information relating to information security and e-PHI.
3. The clinical units will review and update their respective risk analyses and report as requested to the Information Technology Services Information Security Office and Office of Compliance.
4. Clinical units that fail to comply with their obligations under this policy will be reported to the Executive Information Security Committee and to the applicable deans and/or senior management.

Additional References


45 CFR §164.308

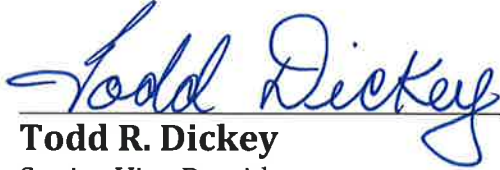
National Institute of Standards and Technology Special Publication (SP) 800-30; 800-66

Responsible Offices:

Information Technology Services
Information Security office
consult@usc.edu
(213) 740-5555

Office of Compliance
<http://ooc.usc.edu/>
complian@usc.edu
(213) 740-8258


Executed by: Michael Quick
Provost and Senior Vice
President, Academic Affairs


Todd R. Dickey
Senior Vice President,
Administration

Date issued: March 1, 2016

| | | |
|--------------|---|---|
| Issued by: | Michael Quick Provost and Senior Vice President, Academic Affairs | Todd R. Dickey Senior Vice President, Administration |
| Date issued: | March 1, 2016 University of Southern California Page 3 of 3 | |