SECURITY ASSESSMENT AND MANAGEMENT

PURPOSE
This policy describes the security assessment procedures to be followed by UCLA Health System and David Geffen School of Medicine at UCLA (hereafter referred to as “UCLA Health”) in evaluating, remediating and managing potential risks to the confidentiality, integrity and availability of Restricted Information (“Security Assessment”) as required by the Administrative Simplification requirements contained in the federal Health Insurance Portability and Accountability Act (referred to as the “Security Rule”) and the University of California Business and Finance Bulletin IS-3, Electronic Information Security.

DEFINITIONS
“Protected health information” or “PHI” is any individually identifiable health information, in any format, including verbal communications. “Individually identifiable” means that the health or medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual’s identity. PHI includes patient billing and health insurance information and applies to a patient’s past, current or future physical or mental health or treatment.

“Electronic Protected Health Information” or “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.

“Personal Information (PI)” as used in this policy is an individual’s first name or first initial and last name combined with any one of the following:

1. social security number,
2. driver’s license number or California identification card number,
3. account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account,
4. medical information, or
5. health insurance information.

“Medical Information” means any information, in either electronic or physical form, regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, and which may be in the possession of or derived from a health care provider, health care service plan, pharmaceutical company or contractor. “Health insurance information” means an
individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. Medical information and health insurance information for patients are also considered to be PHI.

“Restricted Information” (as defined by UC Policy IS-3, Electronic Information Security) describes any confidential or Personal Information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. This includes Personal Information, PHI and ePHI as defined in this section but could also include other types of information such as research data.

“Risk” is the likelihood of a given threat triggering or exploiting a particular vulnerability and the resulting impact on the organization.

“Threat” is the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

“Vulnerability” is a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.

POLICY

I. Introduction

UCLA Health shall conduct ongoing Security Assessments to identify the electronic information resources that require protection and to understand and document risks from potential threats and vulnerabilities to electronic resources that may cause loss of confidentiality, integrity or availability of Restricted Information. Such risk assessments will take into account the potential adverse impact on the University’s reputation, operations and assets. The Security Assessment will be utilized to develop and maintain an ongoing Security Risk Management Plan to identify and reduce ongoing and potential new risks.

II. Security Assessment

UCLA Health will perform ongoing Risk Analysis to accurately and thoroughly assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of the electronic information resources held by the organization. Guidance, central data consolidation and reporting will be provided by the Office of Compliance Services – Information Security, but it is the responsibility of managers at all levels to assure that the relevant risk analysis elements are carried out in their areas.
Risk Analysis Elements

A. Scope
The scope will include an analysis of all risk associated with the creation, use, maintenance, storage and transmission of Restricted Information in all forms of electronic media, such as hard drives, USB drives, CDs, DVDs, or other storage devices, personal digital assistants, transmission media or portable electronic media. Electronic media includes, but is not limited to, a single workstation, networks interconnecting multiple locations, servers and embedded systems with devices.

B. Data Collection
Each department will be responsible for identifying where Restricted Information is stored, received, maintained or transmitted in their areas. Departments must create and maintain a data inventory that specifies the type of Restricted Information, the location, the approximate number of records and a contact person.

C. Identify and Document Potential Threats and Vulnerabilities
The Office of Compliance Services - Information Security working with departmental management, IT groups and MITS security resources will identify and document potential threats and vulnerabilities.

D. Assess Current Security Measures
Departments will be responsible to assess and document security measures used to safeguard Electronic Information Resources in their areas.

E. Determine the Likelihood of Threat Occurrence
The Office of Compliance Services - Information Security working with departmental IT groups and MITS security resources will determine and document the likelihood of threat occurrence.

F. Determine the Potential Impact of Threat Occurrence
The Office of Compliance Services - Information Security working with departmental IT groups and MITS security resources will determine and document the potential impact of threat occurrence. The magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability must be assessed.

Potential impact shall be based on:

i. The amount and types of Restricted Information
ii. The extent of the Workforce with access to the Restricted Information or system.
iii. The level of criticality or overall importance of the Restricted Information or system to the continuing operation and mission of UCLA Health.

G. Finalize Documentation
The Office of Compliance Services - Information Security will finalize the documentation for the risk assessment and report the results to Management. The results provide the basis for the Security Management Plan. In addition, the UC HIPAA Privacy and Security Official(s) will be informed of the completion of all documented risk assessments within thirty (30) days of their completion, and will be provided a copy upon request.

H. Periodic Review and Updates to the Risk Assessment
The risk analysis process will be ongoing. New purchases, projects, requests for new public network addresses, and data downloads should all be assessed for information security issues as early in the process as possible. Risks should be re-evaluated when there are any major changes in the environment, such as system upgrades, changes in equipment, personnel or procedures.

III. Security Management Plan
UCLA Health must implement administrative, physical or technical measures that reduce the risks to its information systems containing e-PHI and restricted information to reasonable and appropriate levels.

A. The data from the risk assessment will be used to conduct a gap analysis of security measures, policies and procedures.

B. The Office of Compliance Services - Information Security will identify remediation opportunities, which may include identification and implementation of policies and procedures, administrative solutions (including training) and technical solutions.

C. Each department will be provided with a copy of the risk assessment from their area along with a gap analysis and suggestions on possible remediation.

D. Departments will be asked to respond with corrective action plans that include timelines for remediation and response.

i. Technical security standards for which the cost is prohibitive to implement or technically impossible to implement must be addressed with alternate security precautions to minimize risk to Restricted Information.
ii. Alternate security precautions must be documented including:
   a. The rationale for the decision to implement the alternate safeguard;
   b. Details of the alternate safeguard implemented; and
   c. Any future plans for achieving compliance with the technical standard.

E. The remediation plan must be approved and signed by the Departmental Administrator or Chief Administrative Officer, and then sent to the Office of Compliance Services - Information Security for review and approval.

F. The Office of Compliance Services - Information Security shall track remediation and provide reports on status to Management.

G. For issues that would be more effectively addressed at an Enterprise-wide level, the Office of Compliance Services - Information Security will work with the Chief Compliance Officer to determine the appropriate governance forum for reporting issues and working on long-term improvement projects.

H. The overall Security Management Plan must be updated as the status changes. There will be an ongoing process to evaluate risks for electronic resources and then mitigate those risks.

IV. Questions

Workforce members who have questions regarding the Security Assessment and Management plan functions in their own departments should check with their local IT group or Chief Administrative Officer. For general questions, contact the Office of Compliance Services - Information Security (InfoSecAll@mednet.ucla.edu).

V. Enforcement

Failure to follow any provisions of this policy may result in disciplinary action, up to and including termination.

VI. Policy Exceptions

Unless an exception process is specified elsewhere in this policy, any exceptions to this policy must be for a valid patient care or business reason and must be approved by the Chief Compliance Officer or his/her designee. The Chief Compliance Officer or designee will consult with the appropriate business, leadership and IT groups in evaluating any proposed exceptions. The exception request form can be found at http://compliance.uclahealth.org/workfiles/PDF2/HIPAA%20Privacy/HIPAA%20Forms/General%20Exception%20Request%20form.pdf
REFERENCES
Health Insurance Portability and Accountability Act, 45 CFR 160-164
University of California Business and Finance Bulletin IS-3, Electronic Information Security
University of California Electronic Communications Policy (ECP)
University of California HIPAA Information Security Policy
National Institute of Standards and Technology Special Publication (SP) 800-3

CONTACT
Chief Privacy Officer, Office of Compliance Services
Chief Information Security Officer, Office of Compliance Services

REVISION HISTORY
Approved: February 22, 2006
Effective Date: April 20, 2005; June 21, 2007
Review Date: July 25, 2012
August 31, 2012

APPROVAL
Health Sciences Enterprise Compliance Oversight Board
Approved 12/11/2010, 06/27/2012

David Feinberg, M.D.
CEO and Associate Vice Chancellor
UCLA Hospital System

Randolph Steadman, M.D.
Chief of Staff
Ronald Reagan UCLA Medical Center

Denise Sur, M.D.
Chief of Staff
Santa Monica-UCLA Medical Center and Orthopaedic Hospital

Ian A. Cook, M.D.
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA