PRIVACY AND INFORMATION SECURITY MONITORING AND AUDITING

PURPOSE
The purpose of this policy is to describe the processes for monitoring and auditing UCLA Health System and David Geffen School of Medicine at UCLA (hereafter referred to as “UCLA Health”) Electronic Information Resources for potential threats and vulnerabilities to the confidentiality, integrity and availability of Restricted Information.

DEFINITIONS
“Electronic Information Resources” includes, but is not limited to, computer equipment (servers, workstations, laptops and other portable computers), mobile devices (iPads, smartphones, digital cameras, etc.) software, storage media (USB drives, DVDs, CDs, magnetic tape, memory cards), networks, and computer accounts providing access to applications, electronic mail, Internet browsing and other services.

“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
privacy and information security monitoring and auditing policy HS 9462

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.

“Persons of Interest” are patients who may require ongoing monitoring of access to their PHI because they are high profile individuals, persons of interest to the media, UCLA employees in highly visible roles and other UCLA employees or any patients that have special concerns about their privacy or have been victims of a previous privacy incident or identity theft.

“Security Incident” is the attempted or successful unauthorized access to, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 C.F.R. section 164.304).

“Workforce” means employees, volunteers, and other persons whose conduct, in the performance of their work for UCLA Health, is under the direct control of UCLA Health or the Regents of the University of California, whether or not UCLA Health pays them. The Workforce includes employees, medical staff, and other health care professionals, agency, temporary and registry personnel, and trainees, housestaff, students and interns, regardless of whether they are UCLA trainees or rotating through UCLA Health facilities from another institution

POLICY & PROCEDURE

I. Electronic systems with Restricted Information will be monitored for external and internal attempts at system disruption, unauthorized access, contamination with malicious software and other intrusion efforts at the network level.

II. Electronic applications containing Restricted Information with the ability to log accesses to the system will implement the auditing functions of the system.

III. Access auditing is a required feature for new software and/or systems containing e-PHI and must be included in contracts and agreements. Applications maintained by Business Associates will also be required to maintain access logs
and to provide access reports when requested by UCLA Health.

IV. UCLA Health shall maintain logs to track access and system configuration changes (syslogs, event logs and other system logs) for systems with e-PHI. Logs should be kept online for a minimum of 4 weeks. Archives of logs should be kept for at least 18 months. If a violation or breach of confidentiality or security is verified, the logs relating to the incident will be maintained for a minimum of 6 years.

V. UCLA Health shall maintain audit logs of access to e-PHI, such as those generated by applications involving patient information, for a minimum of 6 years.

VI. Where feasible, proactive monitors will be implemented to flag access to the e-PHI of Persons of Interest for Office of Compliance Services - Privacy review to ensure appropriateness of access. Routine audits to detect unauthorized access to e-PHI as well as audits in response to specific patient complaints or concerns will be conducted under the direction of the Chief Privacy Officer.

VII. For reporting integrity and availability, audit logs are to be maintained centrally. When this is not feasible, System Administrators are responsible to make sure procedures are in place to ensure the integrity and availability of the audit records.

VIII. For existing legacy systems that do not have audit logs, remediation measures must be implemented and can include measures such as minimizing the number of authorized users to the system, restricting the application to a secure subnet, limiting physical access to the system or application or other reasonable technical and/or physical measures.

IX. Security Incidents will be reported to the UCLA Health Chief Information Security Officer and/or Chief Privacy Officer for review, consultation and evaluation. (Refer to HS Policy No. 9459, “Privacy and Information Security Incident Reporting” and HS Policy No., “Privacy and Information Security Sanctions”).

X. Random periodic audits may be conducted as necessary by authorized personnel to ensure the security, privacy, integrity and availability of all UCLA Health data and information systems and ensure compliance with UCLA Health policies.

Information security audits may include, but are not limited to, inspections and reviews of:

A. User and/or system access to any computing or communication device
B. User access to data and/or information including a review of audit trails
C. Physical inspections of computer equipment, systems, devices, servers, printers, workstations and other devices
D. Interactive monitoring and logging of traffic on Mednet
E. Publicly accessible servers

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

XII. 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

XIII. Questions
Workforce members should consult the Office of Compliance Services - Privacy and Information Security (PrivacyInfoSec@mednet.ucla.edu) if they have any questions on this policy.

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)

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
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