PRIVACY AND INFORMATION SECURITY INCIDENT REPORTING

PURPOSE

The purpose of this policy is to describe the procedures by which Workforce members of UCLA Health System and David Geffen School of Medicine at UCLA (hereafter referred to as "UCLA Health") shall be required to report a Privacy and/or Information Security Incident (as defined herein) to appropriate UCLA Health and/or University officials.

DEFINITIONS

"Protected health information" or "PHI" is any individually identifiable health information, in any format, including verbal communications, regarding a patient created as a consequence of the provision of health care. "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.

"Information Security Incident or 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).

"Privacy Incident" is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to Restricted Information, in any format, including verbal.

POLICY

UCLA Workforce members shall report any suspected Privacy or Information Security Incidents immediately to the Privacy and Information Security Offices (PrivacyInfoSec@mednet.ucla.edu) and their supervisor(s).

I. Privacy and Information Security Incidents

A. Privacy Incidents

California law and the Breach Notification Rule require notification under certain circumstances for the unauthorized access to or unauthorized exposure of specific kinds of Restricted Information, including e-PHI and patient information.

Privacy Incidents can involve Restricted Information in all forms, including electronic, paper and verbal. Privacy Incidents can also be Security Incidents. Examples of possible Privacy Incidents include, but are not limited to:

i. An individual accesses the medical record of a co-worker, colleague, friend, family member, supervisor or celebrity when not authorized to do so.
ii. Faxes, emails or regular mail containing Restricted Information are sent to the wrong people or addresses.
iii. Laptops, USB thumb drives, CDs, DVDs, or backup tapes with unencrypted Restricted Information are lost or stolen.
iv. Workforce members discuss patients in elevators or other public locations.
v. Workforce members tell friends, family, or reporters information about patients or otherwise disclose such information without the patient's authorization.
vi. Restricted Information is posted to public view on websites.
vii. Documents containing Restricted Information are left in conference rooms, cafeterias, parking lots, buses, and other public locations.
viii. Documents containing Restricted Information are thrown away in regular trash or recycling bins and not crosscut shredded.
ix. Patient information is collected for research use without the required approvals and consents.
x. Patient information, including photos, is shared publicly on websites or in brochures, presentations and videos without first obtaining patient consent.

B. Information Security Incidents
The federal Security Rule requires that covered entities (such as UCLA Health System),

"*Identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.*"

(45 C.F.R. 164.308 (a) (6) (i))

C. Security Incidents involve electronic information only. Security Incidents may also be Privacy Incidents. Examples of possible Information Security Incidents include, but are not limited to:

i. Laptops, USB thumb drives, CDs, DVDs, or backup tapes with unencrypted Restricted Information are lost or stolen.
ii. Computer systems are compromised by hackers, viruses or malware.
iii. Copiers, scanners and medical devices are discarded without first securely wiping any Restricted Information.

iv. Unauthorized Access: A person gains logical or physical access without permission to a network, system, application, data, or other resource.
v. Inappropriate Usage: A person violates UCLA Health's acceptable computing use policies.
vi. Shadowing of login and password information and transmission to an unknown outside party.
vii. Corruption of a computer system and/or data.

In order to recognize Privacy and Information Security Incidents, it is important for all UCLA Health Workforce members to familiarize themselves with (and comply with) all University policies, procedures and standards relating to privacy and information security, including these incident reporting procedures.

II. Workforce Member Reporting

Workforce members must immediately notify the Privacy and Security Offices (PrivacyInfoSec@mednet.ucla.edu) and their supervisor when they have any knowledge or even only suspect that a Privacy or Information Security Incident may have occurred. Prompt reporting allows prompt investigation and response for Incidents that could require expert handling and potentially cause harm to the individuals whose information is involved and to UCLA Health. Some Incidents may require notification to external entities, which can have a mandated response time as short as five business days, so immediate reporting of Privacy or Information Security Incidents is essential.

III. Investigation

The Privacy and Information Security Offices will coordinate the investigation of any Privacy and Information Security Incidents following the University of California Privacy and Data Security Incident Response Plan. The Chief Compliance Officer, Chief Information Officer, Chief Privacy Officer, Chief Information Security Officer, Risk Management, Legal Affairs, Media Relations, Human Resources and Law Enforcement will be involved as necessary.

IV. External Reporting

In some cases, California law and federal regulations require notifying regulators and the individuals involved of unauthorized exposure of Restricted Information, The Chief Compliance Officer or his/her designees within the Privacy and Information Security Offices will determine when notification is required. The Privacy and Information Security Offices will coordinate the notification and will involve Legal Affairs and Media Relations as necessary. See: University of California HIPAA Breach Response Policy, UCLA Policy No. 420, *"Notification of Breaches of Computerized Information"*; University of California Business and Finance Bulletin IS-3, Electronic Information Security; and University of California Privacy and Data Security Incident Response Plan.

V. Mitigation

The Privacy and Information Security Offices will work with the Chief Compliance Officer, Legal Affairs, the Chief Information Officer, Human Resources, Risk Management and others as necessary to mitigate any harmful effects that are known to UCLA Health (see: HS Policy No. 9490, *"Mitigation")*

VI. Documentation

The Privacy and Information Security Offices will work with the business units or departments involved in the investigation, external reporting, and mitigation to ensure that Privacy and Information Security Incidents are properly documented.

VII. Enforcement

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

VIII. Questions

Workforce members should consult the Privacy and Information Security Offices (PrivacyInfoSec@mednet.ucla.edu) if they have any questions on this policy.

REFERENCES

Health Insurance Portability and Accountability Act, 45 CFR 160-164
Office for Civil Rights, "Breach Notification for Unsecured Protected Health Information: Interim Final Rule"
http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf
California Medical Information Act, California Civil Code Section 56 *et seq.*
Information Practices Act of 1977, California Civil Code Sections 1798.29 and 1798.82
California Health and Safety Code Section 1280.15
University of California HIPAA Breach Response Policy
University of California Privacy and Data Security Incident Response Plan
University of California Business and Finance Bulletin IS-3, Electronic Information Security
University of California Electronic Communications Policy (ECP)
UCLA Policy No. 420, Notification of Breaches of Computerized Personal Information

CONTACT

Chief Privacy Officer, Compliance Office
Chief Information Security Officer, Compliance Office

REVISION HISTORY

Approved: February 22, 2006
Effective Date: April 20, 2005
Revised: November 2005, March 31, 2011

APPROVAL

Health Sciences Enterprise Compliance Oversight Board
Approved 12/11/2010

David Feinberg, MD
CEO and Associate Vice Chancellor
UCLA Hospital System

Randolph Steadman, MD
Chief of Staff
Ronald Reagan UCLA Medical Center

Denise Sur, MD
Chief of Staff
Santa Monica-UCLA Medical Center and Orthopaedic hospital

James J. McGough, MD
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA