University of California Policy

HIPAA Breach Response

Responsible Officer: Senior Vice President/Chief Compliance and Audit Officer

Responsible Office: Ethics, Compliance and Audit Services

Effective Date: September 13, 2010

Next Review Date: September 1, 2013

Who is Covered: All UC HIPAA workforce members

Contents

Policy Summary

The federal HITECH Act requires the University of California (UC) to notify individuals and the federal Department of Health and Human Services (DHHS) in certain circumstances when Protected Health Information (PHI) is inappropriately used or disclosed.

Policy Definitions

Refer to the document entitled “UC HIPAA Glossary”.

Policy Text

All workforce members of UC's SHCC and SHPC who become aware of or suspect any unauthorized use or disclosure of protected health information (PHI), or a breach in the security of a computerized system containing such information, shall be responsible for reporting such unauthorized access or breach to their supervisor or to the designated Privacy Official. The designated Privacy Official is responsible for immediately notifying the UC HIPAA Privacy Official of all significant[1] incidents. Notification of the appropriate Privacy Official(s) will be made automatically if the designated UCOP electronic case management system (currently *EthicsPoint*) is used to report the incident.

The UC HIPAA Privacy Official, in conjunction with OGC, is responsible for maintaining current documentation regarding applicable state and federal breach notification laws, and making such documentation available to the HIPAA Officers. Revisions shall be made and distributed as soon as practically possible.

The UC HIPAA Privacy Official is responsible for developing, maintaining, periodically reviewing, and updating a UC Privacy Breach Response Plan (Plan), as appropriate. The Plan shall be reviewed and approved by representatives from the Office of General Counsel, Information Resources and Communications, and External Relations in a timely manner.

The Plan shall contain, at a minimum, content to cover the processes of Governance, Triage, Scoping, Execution, and Remediation of incidents.

The HIPAA Officers or their designees are responsible for executing the Plan in the case of any suspected or actual breach that is limited to that HIPAA Officer's covered component. The UC HIPAA Privacy Official or his/her designee is responsible for coordinating the response for any suspected or actual incident that spans more than one covered component.

The HIPAA Officer shall consult with the UC HIPAA Privacy Official prior to notification of any major media outlets or state or federal agencies, and allow sufficient time for UCOP internal consultation, without jeopardizing any regulatory obligations.

Each HIPAA Officer shall report to the UC HIPAA Privacy Official on a periodic basis (as defined by the UC HIPAA Privacy Official), but no less frequently than annually by calendar year-end, summary information (as defined by the UC HIPAA Privacy Official) about breaches within his/her respective covered component.

Approval Authority

Implementation of the Policy: Senior Vice President/Chief Compliance and Audit Officer

[1] "Significant" incidents are any incidents or potential incidents that require or may require notification to individuals and/or regulatory agencies and/or the media and/or law enforcement. Generally speaking, incidents involving a single patient, such as a misdirected fax, are not considered significant, but they may be, depending on the circumstances, such as inappropriate access of a high-profile public figure's records. A more detailed discussion of "significant" incidents is found in the *UC Privacy and Data Security Incident Response Plan*.

Revisions to the Policy: Senior Vice President/Chief Compliance and Audit Officer

Approval of Actions: not applicable

Compliance and Reporting

N/A

Implementation Procedures

UC Organizational Units subject to HIPAA are responsible for implementation.

Related Documents

45 CFR 164.404

UC Privacy and Data Security Incident Response Plan

Business and Finance Bulletin IS-3, *Electronic Information Security*

Frequently Asked Questions

FAQs may be found on the UC HIPAA website.

Revision History

Version 1