Topic
Business Administration [1]
Policy Number
200-30
Reviewed Date
March 28, 2012
Responsible Office

- Office of the Executive Vice Chancellor and Provost [2]

Purpose
To define the authority and responsibility for the UCSF response in relation to a potential or actual privacy breach of Protected Health Information (PHI), Medical Information or Health Insurance Information, and to delineate the Privacy Investigation response process.
Definitions

Covered Entity (CE)

An entity that must comply with HIPAA. The term Covered Entity refers to health care providers, health plans, and health care clearing houses that perform a covered service and transmit data electronically.

Health Insurance Information

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. [California Civil Code Sec. 1798.82]

HIPAA

The Health Insurance Portability and Accountability Act of 1996. A federal privacy law.

HITECH

The Health Information Technology for Economic and Clinical Health Act, or HITECH Act, amends the HIPAA regulations and is part of the American Recovery and Reinvestment Act of 2009 aka ?the Stimulus Bill.?

Hybrid Entity

A single legal entity that is a covered entity, whose business activities include both covered and non-covered functions; and that designates health care components. The University is a single Hybrid Entity. [45 CFR § 160.103]

Licensed Facility

A clinic, health facility, home health agency, or hospice licensed pursuant to sections 1204, 1250, 1725, or 1745 of the California Health and Safety Code. For the purposes of this policy, the unauthorized access notification requirements of Health & Safety Code Sec. 1280.15 only apply to Licensed Facilities. [California Health and Safety Code Sec. 1280.15, as amended by SB 541]

Medical Information

Any individually identifiable information, in electronic or physical form, that is in the possession of, or derived from, a provider of health care, health care service plan, pharmaceutical company or contractor, regarding a patient?s medical history, mental or physical condition, or medical treatment, or diagnosis. ?Individually identifiable? means that the 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, SSN, or other information that, alone or in combination with other publicly available information, reveals the individual?s identity. [CMIA, California Civil Code 56.05]

Privacy Breach

The unauthorized or inappropriate acquisition, access, use or disclosure of unsecured PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Breach does not include the following circumstances:
Any intentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if (i) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and employee or individual, respectively, with the covered entity or business associate; and (ii) such information is not further acquired, accessed, used, or disclosed by any person
Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated

individual at the same facility; and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person
A situation in which an unauthorized person to whom the information is disclosed would not reasonably be able to retain the information (e.g., PHI that was sent out by the post office is returned unopened, as undeliverable)

Protected Health Information (PHI)

Any individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Records covered by the Family Educational Rights and Privacy Act of 1974 (FERPA) are excluded from the definition of PHI.

Policy

A. Governance Structure and Chief Privacy Officer (CPO):

Federal regulations mandate the development of a privacy governance structure which includes the appointment of a Chief Privacy Officer, who is responsible for the development, implementation of, and adherence to, the policies and procedures necessary to ensure compliance. At UCSF, the Chief Privacy Officer (CPO) is designated by the Chancellor and the Medical Center CEO.

UCSF?s privacy response governance structure designates covered components and the required response elements for a Privacy Investigation up to and including determination of a breach and notification.

B. Covered Components:

The University is a single hybrid entity. UCSF?s designated health care covered components are: the Medical Center, Langley Porter Psychiatric Institute, and Proctor Foundation. The School of Dentistry, School of Medicine, School of Nursing, School of Pharmacy, UCSF Fresno, Student Health Services, Development Office, University Relations and Clinical Research areas contain both covered and non-covered components.

The covered components of UCSF comply with state and federal privacy and confidentiality laws.

C. Breach

In the event of a privacy breach, the HITECH Act and other federal and state laws and regulations require UCSF to notify affected individuals, and based on the information used or disclosed, the federal Department of Health and Human Services (DHHS) and/or the California Department of Public Health (CDPH).

Responsibilities

A. Authority

1. The Privacy Office is the office of record responsible for the coordination of privacy investigations and, in conjunction with the Privacy, Legal and Risk team (PLR) and UCOP as appropriate, the determination of whether notification for breaches of PHI, Medical Information and Health Insurance Information is appropriate. (Appendix A [3])

2. The Privacy Compliance Steering Committee (PCSC) is comprised of Senior Leaders from across the UCSF Enterprise and functions as an approving body and a communication link to the respective areas, schools or departments at UCSF as follows: a. Provides general oversight for:

i. All HIPAA rules: Privacy, Security, National Provider Identifier, Transaction Codes, Enforcement and Civil Monetary Penalties and the HITECH act

ii. Other related State Privacy Legislation, including SB1386 [Ch. 915], AB1298 [Ch. 699], Lanterman Petris Short Act [Welfare and Institutions Code Section 5328 et seq.], SB541 [Ch. 605] & AB211 [Ch. 602], and CMIA [Civil Code Section 56, et seq.]

b. Supports the mandated responsibility to keep UCSF?s Senior Leadership apprised of the organization?s compliance progress and status related to privacy compliance regulations

c. The PCSC reports to:

i. Ethics Compliance Board, which reports to the Chancellor

ii. Executive Medical Board

iii. Governance Advisory Council

3. Privacy, Legal and Risk team (PLR): plays a key advisory role in determining notifications for complex incidents.

B. Reporting Responsibilities:

1. Any UCSF workforce member, who becomes aware of or suspects any inappropriate use or disclosure of PHI, is responsible for immediately reporting this knowledge to their supervisor or to the Privacy Office (415) 353-2750.

2. When an incident involving a lost or stolen electronic device is reported to IT, IT Security is responsible for immediate notification of the Privacy Office.

3. The Chief Privacy Officer (CPO) is responsible for notifying the UCSF Chief Ethics and Compliance Officer (CECO) and the UC System-wide Senior Vice President (SVP) for Compliance and Audit or designee of any significant or high visibility incident. The SVP for Compliance and Audit will then notify key UCOP personnel.

C. Investigative Process (See Appendix A [3]):

1. The Privacy Office receives allegations of non-compliance and violations of patient privacy regulations from all areas across the UCSF enterprise and from external sources.

2. When the Privacy Office receives notification of a suspected or known privacy incident, the CPO or their designee will work with the department in which the alleged violation occurred to investigate and gather the factual details.

3. Based on a determination of the potential size and significance of the privacy violation, the CPO will alert PLR, UCSF Senior Leadership (PCSC) and UCOP. The CPO may then opt to utilize a vendor to perform or assist with any of the following steps including investigation, electronic data analysis, containment, notification, and remediation.

4. If electronic data analysis is required, either UCSF IT Security or the vendor will perform a forensic analysis and scan for PHI on all back up files and emails. The results of the analysis and scans will be immediately provided to the Privacy Office. The Privacy Office will coordinate with the affected department to determine the type and purpose of the information. The Privacy Office will review the factual details to determine whether unauthorized access of PHI consistent with federal and state laws and regulations has occurred.

D. Notifications:

1. Based on an analysis of the factual data, and in consultation with PLR, CECO, UCSF Executive Leadership, and UCOP as appropriate (Appendix A [3]), the Privacy Office will make a determination as to whether notification is necessary.

2. For electronic cases, the CPO and ISO will coordinate an assessment of whether to disrupt systems and services as appropriate when warranted by the nature of the privacy breach. If warranted, the decision will be made in consultation with the appropriate senior leadership and must take into consideration the impact on critical patient care or life-support services.

3. The Privacy Office will oversee the notification process for any PHI breach. The Privacy Office may:

a. Identify the victims of the breach and cross reference with data lists to compile the most recent contact addresses

b. Develop an internal and external communication plan:

i. Chancellor, Privacy Steering Committee, I Group, UCOP, ECB, others

ii. External Regulatory agencies

iii. Media notification is the responsibility of Public Affairs (the Privacy Office will collaborate with Public Affairs regarding internal and external communication)

iv. Affected Individuals

c. Notify appropriate Regulatory agencies:

i. Each Regulatory Agency will be provided with the required information in the appropriate format and manner required by law or regulation

ii. The timing of notification will be determined in accordance with Regulatory Agency requirements

d. Select and identify notification methods for affected individuals

e. Draft, finalize and determine who will sign the notification letter

f. Develop FAQs

g. Post a website notice in conjunction with Marketing/Public Affairs

h. Activate a Call Center and develop a script for Call Center Staff

i. Take any other necessary action

E. Remediation:

1. The Privacy Office is responsible for providing oversight and advisory assistance to the senior leadership of the affected department to ensure that appropriate remediation occurs. This process may include, but is not limited to the following:

a. Identification of areas where different processes, technical measures, and/or individual monitoring might have prevented the privacy breach

b. Implementation and ongoing monitoring of process changes, technical measures, or individual disciplinary measures designed to prevent a breach in the future

c. Performance of a root cause analysis as necessary

Related Policies

- 650-16 - Information Security and Confidentiality [4]

References

- California Confidentiality of Medical Information Act (CMIA) [Civil Code Section 56, et seq.] [5]
- California Senate Bill 1386 [Civil Code 1798.82, [6] 1798.29] [7]
- Health Insurance and Portability Act (HIPAA) [Title 45 Code of Federal Regulations Part 160, [8] 162 [9] and 164] [10]
- Health Information and Technology for Economic and Clinical Health (HITECH) Act [Title XIII, Division A, ARRA] [11]
- Information Practices Act of 1977 (IPA) [California Civil Code Section 1798 et seq.] [12]
- Lanterman-Petris-Short Act (LPS) [Welfare and Institutions Code Section 5328 et seq.] [13]
- UCOP HIPAA Breach Response (9/13/2010) [14]
- UCOP Privacy and Data Security Incident Response Plan (12/1/2011) [15]
- UCOP Information Breach Decision Tree for California State Law (12/21/2011) [16]
- UCOP Business and Finance Bulletin IS-3 Electronic Information Security [17]
- UCSF Privacy Handbook [18]

Links
[1] https://policies.ucsf.edu/policy/200
[2] mailto:ExecutiveViceChancellor@ucsf.edu
[3] https://policies.ucsf.edu/sites/policies.ucsf.edu/files/200-30%20Privacy%20Investigation%20Policy%20Appendix%20A%20032912%20.pdf
[4] https://policies.ucsf.edu/policy/650-16
[5] http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20
[6] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84
[7] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29
[8] http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr160_main_02.tpl
[9] http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr162_main_02.tpl
[10] http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
[11] http://www.law.cornell.edu/uscode/text/42/chapter-156/subchapter-III/part-A
[12] http://www.leginfo.ca.gov/.html/civ_table_of_contents.html
[13] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=wic&group=05001-06000&file=5325-5337
[14] http://policy.ucop.edu/doc/1110162/HIPAA-5
[15] http://www.ucop.edu/information-technology-services/_files/uc_incidentresp_plan.pdf
[16] http://www.ucop.edu/information-technology-services/initiatives/university-policies/ucinfo_breach_decision_tree_ca_state_law.pdf
[17] http://policy.ucop.edu/doc/7000543/BFB-IS-3
[18] http://hipaa.ucsf.edu/Privacy_Handbook.pdf