Topic
Information Technology [1]
Policy Number
650-16
Reviewed Date
October 11, 2017
Responsible Office

- Office of the Senior Vice Chancellor, Finance and Administration [2]

Purpose

The purpose of this policy is to provide for compliance with federal and state law and regulation and university policy governing the security and confidentiality of electronic information.

Definitions

Access Control

The policies and procedures that regulate Authorized Users? ability or means necessary to read, write, modify, or communicate data or information or otherwise use any Electronic Information Resource (EIR).

Authorized User

Any UCSF faculty, staff, student, or other individual affiliated with UCSF who has been granted authorization to access an Electronic Information Resource or invokes or accesses an Electronic Information Resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with UCSF. The authorization granted is for a specific level of access to the Electronic Information Resource in accordance with University policy. An example of an Authorized User is someone who handles business transactions and performs data entry into a business application or someone who gathers information from an application or data source for the purposes of analysis and management reporting.

Confidentiality

The degree to which data or information is not available or disclosed to unauthorized persons or processes. The degree of confidentiality afforded to different types of information will vary in accordance with the requirements of federal and state laws, University policy, contract, or community practice. (See Information Classifications)

Compromise

Unauthorized (actual or suspected) access, use, disclosure, modification, or destruction of an Electronic Information Resource in violation of University policy.

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.

Electronic Information Resource (EIR)

A resource used in support of UCSF activities that involve the electronic storage, processing, or transmitting of data as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, and data?in raw, summary, and interpreted form?and associated computer server, desktop, communications, and other hardware used in support of UCSF activities. Personally owned systems are included in this definition if they connect to the UCSF network or are used to process or store UCSF information.

Information Classifications

The UCSF Data Classification Standard (Addendum F) [3] defines categories according to their unique protective requirements and provides guidance for identifying appropriate users or recipients. UCSF departments and units should determine in advance the extent to which information should be disclosed to specific users. Determinations should be made based on the nature of the content and the duties of department employees.

Licensed Information Resources

Licensed Information Resources refer to paid online resources (e.g., databases, journals,

books) licensed by the UCSF Library for access and use by the UCSF community only.

Minimum Security Standards For Electronic Information Resources (EIR)

The UCSF Minimum Security Standards for EIRs are required to protect all UCSF EIRs. Development of these standards is the responsibility of the Information Security Committee. Their implementation is the joint responsibility of Technical Support Providers and Authorized Users. Departmental Officials and IT are responsible for assuring that the minimum standards are implemented within their sphere of influence. The minimum standards shall be reviewed and modified by the Information Security Committee as needed to respond to emerging technologies and organization changes, but no less frequently than annually. (Addendum B)

Security Incident

The attempted or successful unauthorized access, use, disclosure, modification, or destruction of an Electronic Information Resource in violation of University policies.

Security Threat

Any action by an individual or application that may result in a security incident and compromise the confidentiality, integrity, or availability of data. Threats that could breach confidentially include, but are not limited to, unauthorized intrusions, malicious misuse, inadvertent compromise, viruses, or the loss or theft of a computing device that contains restricted or sensitive information, or any incident in which a user either directly or by using a program performs functions for which they do not have authorization.

UCSF Users/Workforce Members

UCSF students, faculty, staff, and others affiliated with the University (including those in program, contract, or license relationships with the University) who need to access restricted or sensitive information and have authorization to use University Electronic Information Resources and services for purposes in accordance with The Electronic Communications Policy [4], Section III.D, Allowable Uses. (See Authorized User)

Policy

UCSF will protect the confidentiality, integrity, and availability of restricted or sensitive information, when such information is created, received, transmitted, and/or stored in any medium, including electronic or paper format, and will ensure that the handling of such information is consistent with federal and state laws and regulations and university policies.

Each member of the campus community is responsible for the security and protection of EIRs over which he or she has control. UCSF Minimum Security Standards for Electronic Information Resources (Addendum B) [5] has been published to help departments and individuals protect their computing devices. UCSF Wireless Networks [6] is published to assist in providing comprehensive protection of the wireless extension of UCSF networks (Addendum D [6]). Likewise, within the UCSF distributive computing environment, the IT Governance Committee and Information Security Committee have identified specific roles and responsibilities for securing EIRs UCSF Roles and Responsibilities for Securing Electronic Information Resources (Addendum A) [7]. UCSF data that is lost, stolen, compromised, or suspected of being compromised must be reported and investigated according to UCSF Incident Investigation (Addendum C) [8]. UCSF users/workforce members who handle or process credit card information must adhere to the PCI Standard (Addendum E) [9]. UCSF shall utilize the UCSF Data Classification Standard (Addendum F) [3] to determine the assigned classification of information by data type, protection level, availability level, legal requirements, access requirements, and encryption requirements. Any third party that remotely accesses UCSF resources or the UCSF network as well as UCSF business units and departments that sponsor or manage third parties who remotely access UCSF resources or the UCSF network, shall follow the Third Party Remote Access Standard (Addendum G) [10].

Responsibilities

Contact Responsible Office (above) with any questions.

References

- UCSF Privacy and Confidentiality Handbook (HIPAA) [11]
- UCSF Privacy & Confidentiality Website (HIPAA) [12]
- UCSF Information Technology [13]
- University of California HIPAA Website [14]
- UC Information Technology Services [15]
- Addendum A, UCSF Roles and Responsibilities for Securing Electronic Information Resources [7]
- Addendum B, UCSF Minimum Security Standards for Electronic Information Resources [5]
- Addendum C, UCSF Incident Investigation [8]
- Addendum D, UCSF Wireless Networks [6]
- Addendum E, PCI [9]
- Addendum F, UCSF Data Classification Standard [3]
- Addendum G, 3rd Party Remote Access [16]
- U.S. Department of Health & Human Services (HHS) ? Health Information Privacy [17]

Links
[1] https://policies.ucsf.edu/policy/650
[2] mailto:SVCPOLICIES@ucsf.edu
[3] https://it.ucsf.edu/policies/dataclassification
[4] http://policy.ucop.edu/doc/7000470/ElectronicCommunications
[5] http://it.ucsf.edu/policies/ucsf-650-16-addendum-b-ucsf-minimum-security-standards-electronic-information-resources
[6] http://it.ucsf.edu/policies/ucsf-650-16-addendum-d-wireless-networks
[7] http://it.ucsf.edu/policies/ucsf-650-16-addendum-ucsf-roles-and-responsibilities-securing-electronic-information-resour
[8] http://it.ucsf.edu/policies/ucsf-650-16-addendum-c-ucsf-incident-investigation
[9] http://it.ucsf.edu/policies/ucsf-650-16-addendum-e-pci
[10] http://it.ucsf.edu/policies/ucsf-650-16-addendum-g-3rd-party-remote-access-standards
[11] http://hipaa.ucsf.edu/sites/hipaa.ucsf.edu/files/UCSFPrivacyConfidentialityHandbook2015.pdf
[12] http://hipaa.ucsf.edu
[13] http://it.ucsf.edu/
[14] http://www.universityofcalifornia.edu/hipaa/welcome.html
[15] http://www.ucop.edu/information-technology-services/initiatives/uc-information-security/index.html
[16] http://it.ucsf.edu/policies/3rd-party-remote-access-standards
[17] http://www.hhs.gov/hipaa/index.html