Published on Campus Administrative Policies (https://policies.ucsf.edu)

Home > Information Security and Confidentiality

**Topic**
Information Technology [1]

**Policy Number**
650-16

**Reviewed Date**
May 8, 2020

**Purpose**

The purpose of this policy is to provide for compliance with federal and state law and regulations 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 Institutional Information.

**Authorized User**

Any UCSF faculty, staff, student, or other individual affiliated with UCSF who has been granted authorization to access or invoke Institutional Information 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 Institutional Information 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.

Institutional Information

A term that broadly describes all data and information created, received and/or collected by UC. The UCSF Data Classification Standard (Addendum F) 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 Institutional Information

The UCSF Minimum Security Standards for Institutional Information are required to protect all UCSF IT Resources. 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 Committee on IT Security as needed to respond to emerging technologies and organization changes. (Addendum B)

Security Incident
The attempted or successful unauthorized access, use, disclosure, modification, or destruction of Institutional Information 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 confidentiality 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 [3], 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 Institutional Information over which he or she has control. UCSF Minimum Security Standards for Electronic Information Resources (Addendum B) [4] has been published to help departments and individuals protect their computing devices. UCSF Wireless Networks [5] is published to assist in providing comprehensive protection of the wireless extension of UCSF networks (Addendum D [5]). Likewise, within the UCSF distributive computing environment, the IT Governance Steering Committee and Committee on IT Security Technical Workgroup have identified specific roles and responsibilities for securing Institutional Information within UCSF Roles and Responsibilities for Securing Electronic Information Resources (Addendum A) [6]. UCSF data that is lost, stolen, compromised, or suspected of being compromised must be reported and investigated according to UCSF Incident Investigation (Addendum C) [7]. UCSF users/workforce members who handle or process credit card information must adhere to the PCI Standard (Addendum E) [8]. UCSF shall utilize the UCSF Data Classification Standard (Addendum F) [2] 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) [9].

Responsibilities

Contact Responsible Office (above) with any questions.

References

- UCSF Privacy and Confidentiality Handbook (HIPAA) [10]
- UCSF Privacy & Confidentiality Website (HIPAA) [11]
- UCSF Information Technology [12]
- University of California HIPAA Website [13]
- UC Information Technology Services [14]
- Addendum C, UCSF Incident Investigation [7]
- Addendum D, UCSF Wireless Networks [5]
- Addendum E, PCI [8]
- Addendum F, UCSF Data Classification Standard [2]
- U.S. Department of Health & Human Services (HHS) ? Health Information Privacy [16]