Patients of the University of California, San Francisco (UCSF) have both a reasonable and legal right to the privacy and confidentiality of their personal health information. As such, UCSF has patient privacy and confidentiality policies and procedures in place to guide and direct the workforce on appropriate access, use and disclosure of patients’ protected health information. This policy describes the sanctions to be taken by UCSF when workforce members fail to comply with the patient privacy and confidentiality policies and procedures of the University of California and UCSF. This policy applies to any patient health information obtained and/or used inappropriately during the course and scope of work at UCSF. In addition to the corrective action defined in this policy, fines may be imposed by regulatory agencies, and civil actions by third parties outside of UCSF may be undertaken against UCSF workforce members.

Definitions

Business Associate (BA)

A person or entity, not a part of a Covered Entity’s workforce, that on behalf of the Covered Entity: 1) participates in, performs, or assists in the performance of a function or activity involving the use or disclosure of PHI; or 2) provides services to or for the Covered Entity, where the provision of the service involves the disclosure of PHI to the BA. BA functions and activities may include, but are not limited to, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Business Associate services may include, but are not limited to, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation and financial services.

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.

Workforce

Employees, volunteers and other persons whose conduct, in the performance of their work for
UCSF, is under the direct control of UCSF or The Regents of the University of California,
whether or not UCSF pays them. The workforce includes faculty, non-faculty academics, staff,
students, trainees, vendors and volunteers, and it includes those who are rotating through
UCSF’s facilities from another institution, as well as those who are employed by an affiliated
institution, who in the course of their duties need to access patient health information.

Policy

A. In accordance with standard UC policies, rules, regulations and laws, the University may
initiate corrective action, up to and including termination or release during probation,
when a workforce member has violated UCSF patient privacy or confidentiality policies
and procedures. The initiation of any corrective action by the University does not
preclude the University from seeking any other remedy available to it under law.
B. Should the University initiate any corrective action, it must do so in accordance with the
applicable workforce policies and/or union contracts which may include, but are not
limited to, the Faculty Code of Conduct, University of California Policies Applying to
Campus Activities, Organizations and Students, the Medical Staff Bylaws, Medical Staff
Rules and Regulations, Graduate Medical Education (GME) policies and procedures, as
well as any other existing and applicable policies for staff, collective bargaining
agreements, University policies or practices, as applicable.
C. The corrective action imposed will depend on the nature, severity and frequency of the
violation, as appropriate to the policies governing the workforce member.
D. The University retains the right to pursue collection from the workforce member for the
costs, direct or indirect, incurred by the University associated with the privacy breach
investigation and legal defense processes (e.g., forensic scans, attorney fees), as well
as fines and/or administrative penalties imposed against the University, for privacy
violations caused by the workforce member. Factors for determining the workforce
member’s liability for such costs include, but are not limited to, existence of malicious
intent and/or whether the violation was a result of an egregious disregard to policies and
procedures.

Responsibilities

A. UCSF may initiate disciplinary actions in cases of misconduct, repeated violations, or
otherwise consistent with University policies.
B. Workforce members should review the policies listed in Policy Section B for a
comprehensive description of the disciplinary policies and procedures, including their
rights under such circumstances.
C. The Privacy Office will investigate, in consultation with all applicable offices, all cases of
alleged non-compliance with UCSF’s patient privacy and confidentiality policies. Cases for which sanctions may be appropriate will be referred to the applicable office for review as appropriate to the policies and procedures governing the workforce member. Relevant laws, regulations and UCSF’s policies and procedures will be considered.

D. For Business Associates and other vendors, the Privacy Office and Information Security Office (if electronic information resources are involved) will work with the appropriate UCSF department to implement any compliance corrective action or recommend appropriate sanctions.

E. Any sanctions that are applied will be documented by the appropriate governing body for the workforce member involved. Any appropriate sanctions for contractors and Business Associates will be documented by the Privacy Office and Information Security Office (if electronic information resources are involved).

Related Policies

- 200-30 - Privacy Investigation Policy
- 650-16 - Information Security and Confidentiality
- 200-28 - HIPAA Business Associates
- 150-23 - Reporting Improper Governmental Activities and Protection Against Retaliation (Whistleblower Policy & Whistleblower Protection Policy)

References

- Confidentiality, Access, Use and Disclosure of Protected Health Information and Patient Privacy 5.02.01
- Control of Access and Release of Information from UCSF Medical Center Information Systems for Research Purposes 5.01.06
- Information Security and Confidentiality 5.01.04
- Electronic Mail 5.01.02
- Code of Conduct and Principles of Compliance 1.02.09
- Facsimile Documents Containing PHI 5.01.25
- HIPAA Business Associates 1.02.15
- Health Insurance and Portability Act (HIPAA) [Title 45 Code of Federal Regulations Part 160, 162 and 164]
- University of California HIPAA Administrative Requirements
- University of California Business & Finance Bulletin IS-3, Electronic Information Security
- University of California Electronic Communications Policy (ECP)
- University of California Faculty Code of Conduct (APM-015) and University Policy on Faculty Conduct and the Administration of Discipline (APM-016)
- University of California Professional and Support Staff, Disciplinary & Separation Actions, Policies
- UCSF Campus Code of Conduct
- UCSF Medical Staff Bylaws and Rules and Regulations
- University of California Policies Applying to Campus Activities, Organizations and Students
- University of California Policies Applying to Campus Activities, Organizations and Students, including UCSF Campus Supplement
- UCSF Interim Procedure for Investigation of Faculty Misconduct and the Administration of Discipline
- Collective Bargaining Units and Agreements