Purpose

The University of California, as a covered entity under the Health Insurance Portability and Accountability Act (HIPAA), is required to assure that any Business Associate with whom it shares protected health information (PHI) handles that information in accordance with federal and state laws and regulations, including HIPAA. The purpose of this policy is to set forth the requirements necessary to document the UCSF campus’ efforts to assure that Business Associates, agents, and subcontractors comply with HIPAA privacy standards and that the Campus or Medical Center knows about, and has the opportunity to take remedial action regarding, any breach of duty by a Business Associate.

This document is intended for use by the University of California, San Francisco (UCSF) Campus and Medical Center staff and personnel and no representations or warranties are made for outside use. Not for outside reproduction, distribution or publication without the written permission of The Regents of the University of California.

Definitions

Accounting of Disclosures

A required record, made in response to a patient’s request, of all disclosures of PHI made to outside entities within the six years prior to the request date including, but not limited to, disclosures made during a research protocol pursuant to a Committee on Human Research (CHR)/Internal Review Board (IRB) approved Waiver of Authorization.

Business Associate (BA)

A person or entity, not part of the workforce, who/that on behalf of UCSF: 1) participates in, performs or assists in the performance of a function or activity involving the use or disclosure of PHI, or 2) creates, receives, maintains, or transmits PHI. This includes specific categories of organizations such as health information organizations (?HIOs?), e-prescribing gateways, patient safety organizations, and data storage vendors that maintain PHI, even if access to PHI is limited or non-existent.
Business Associate Agreement (BAA)

A written contract between a BA and a covered entity that specifies the permitted uses and disclosures and the safeguards required for Protected Health Information (PHI) by a BA in order to perform a function or activity, or to provide a service on behalf of the covered entity.

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.

Disclosure

The act of releasing, transferring, providing access to, or divulging in any other manner, information outside of the entity holding the information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

A federal privacy law.

Protected Health Information (PHI)

As defined by the Health Insurance Portability and Accountability Act (HIPAA), an individual's health information or data collected from an individual that is created or received by a health care provider, plan or clearinghouse related to the past, present or future physical or mental health or condition of an individual, the provision of health care to the individual; identifies or could reasonably identify the individual; and is transmitted or maintained in electronic or any other form or medium.

Provider
A person or entity that provides medical services and that bills for or is paid for medical services in the normal course of business.

Research Health Information (RHI)

Personally identifiable health information of a human subject arising from biomedical or behavioral research that is neither associated with health care services nor provided in a setting that bills for care. A researcher engaged in interventional clinical studies (i.e., research comparing the safety and effectiveness of a treatment in a setting where services are billed to an insurer) creates PHI.

Treatment, Payment, Health Care Operations (TPO)

The use and disclosure of PHI for purposes of TPO is allowed without a specific Authorization from the patient. Treatment means the provision, coordination and management of health care and related services by one or more health care providers. Examples of treatment include: consultation between health care providers regarding a patient or; referral of a patient to another provider for health care. Payment includes activities undertaken by a provider to obtain reimbursement for health care services, and by a health plan to determine eligibility for coverage and/or provide benefits. Health Care Operations encompass a variety of activities of a covered entity including, but not limited to, quality assessment and improvement, outcome evaluation and development of clinical guidelines, reviewing competence, qualifications, and performance of health care professionals, conducting health care practitioner training programs, accreditation, certification, licensing and credentialing. Note: Use and disclosure of PHI for research purposes requires either a Waiver of Authorization from the IRB or written authorization from the patient

Use

With respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within the entity that maintains such information.

Policy

It is the policy of UCSF that PHI may be disclosed to and used by Business Associates as necessary to allow the BA to carry out a health care-related function or activity on behalf of, or to provide services to, UCSF. A BA must sign a BAA with either the Medical Center or Campus or both, in order to access, use or disclose PHI. The BAA must be in writing and must contain UCSF-approved HIPAA compliant language and authorized signatures.

If UCSF determines that a BA has violated a material term or obligation of the BAA, the department that is party to the agreement and/or the UCSF Privacy Officer shall be notified.
and shall seek to remedy the breach or, if that is not possible, to terminate the agreement. Violations by a BA also may be reported by UCSF to the UC HIPAA Compliance Office and the Secretary of the U.S. Department of Health & Human Services (DHHS).

It is the responsibility of each UCSF Campus or Medical Center department, division, or operating unit contracting for services with a third party to assure that a valid BAA is in place before any PHI is released to the BA.

Campus Low Value Procurements: The BAA shall be added to or included in all commitment and/or procurement documents under which PHI will be released to a BA. PHI shall not be disclosed when using a Request for Delivery/ Purchase Order Release form under any Departmental Low Value Purchasing Authority (LVPA). Any transaction, regardless of value, shall be conducted under a procurement document issued by Campus Purchasing that clearly identifies permitted/intended uses of the PHI to be disclosed. Inclusion of the BAA in a commitment or procurement document may be accomplished by physical amendment or by reference to a master BAA.

This Policy was written in March 2003 and revised in May 2004 to meet HIPAA requirements and has been reviewed by the Office of Legal Affairs, the Business Associates Subcommittee of the HIPAA Steering Committee, the Executive Medical Board, and Office of the Senior Vice Chancellor for Finance - Administration.

This policy will be reviewed every (3) three years or as required by change in law or practice. Departments providing initial approval must approve any changes to the policy.

Responsibilities

A. Department / Division Responsibility: Consistent with the Low Value Purchasing restriction stated above, it is the responsibility of each UCSF department, division, or operating unit in collaboration with Campus or Medical Center Purchasing Departments, when contracting for services with third parties to whom PHI will be shared, to assure that a valid BAA is executed before authorizing or receiving services. If it is not clear whether a contract creates a BA relationship, the contract should be referred for review to the Director, Medical Center Materiel Services, or the Campus Purchasing Manager/Associate Director. UCSF has no obligation to monitor the activities or practices of the BA, but may request additional information or assurances from the BA, including:

1. requesting a copy of the BA’s current security and privacy policies, and including these with the BAA;

2. confirmation with the BA that all subcontractors have executed written agreements to protect the integrity and confidentiality of PHI received from the BA;

3. confirmation that the BA’s employees and subcontractors have been trained to protect the confidentiality of any PHI accessed pursuant to the contract;

4. confirmation that the BA has a contingency plan in place that provides for a (i) one-year data back-up plan; (ii) disaster recovery plan; and (iii) emergency mode of operation plan; and/or
5. confirmation that the BA has written policies and procedures establishing rules for granting access to PHI.

**B. Responsibilities of the BA:** The BAA sets forth the actions for which the BA will be responsible, including:

1. **Permitted Uses of PHI:** The BA may only use or disclose PHI as permitted by the agreement or required by law.

2. **Safeguards:** The BA must use appropriate safeguards to protect the confidentiality of the information and to prevent use or disclosure other than as provided in the contract.

3. **Reporting to the CE:** The BA must report to the CE any use or disclosure not permitted by the contract.

4. **Obligations of Subcontractors:** The BA must ensure that any subcontractor or agent receiving PHI from the BA agrees to the same restrictions and conditions that apply to the BA.

5. **Patient Access to PHI:** The BA must make available to the CE or a patient, upon request, any PHI or other information necessary for the CE to comply with a patient’s rights to access, amend and receive an accounting of disclosures of their PHI.

6. **Secretary to DHHS:** The BA must make PHI available to the Secretary of the DHHS, PHI and the BA’s internal practices, books and records relating to the use and disclosure of PHI.

7. **Return or Destroy PHI:** Once the contract is terminated, the BA must return or destroy the PHI received. If it is not possible to return or destroy the PHI because of other obligations or legal requirements, the protections of the BAA must remain in effect until the PHI is returned or destroyed. No other uses or disclosures of the PHI may be made by the BA other than for the purpose(s) that originally prevented the return or destruction of the information.

**C. Exceptions that do not require a BAA:** A BAA is not required in the following circumstances:

1. disclosures for treatment purposes;
2. disclosures for financial transactions;
3. disclosures between group health plans and plan sponsor;
4. disclosures among the CE’s workforce members for TPO;
5. disclosures of PHI where any access to PHI would be incidental, if at all, and could not reasonably be prevented;
6. disclosures to couriers where the person is a conduit of or carrier for PHI (including both private couriers and their electronic equivalents);
7. software vendors, provided the contract does not require the individual or entity to access PHI in order to provide the vendor service or to verify/validate;
8. disclosures among CEs who participate in an organized health care arrangement (OCHA);
9. disclosures of PHI to researchers for research purposes, provided that appropriate consent and Waiver or Authorization have been obtained from the patient subjects; and
10. disclosures of PHI between UCSF and affiliated training institutions as necessary to carry out training and educational programs, as well as to meet the accreditation requirements of each institution.

**D. Exceptions for Data Aggregation Services:** Generally, a BA is prohibited from using or disclosing PHI in a manner that would be prohibited if done by the CE. A BA is permitted to provide data aggregation services relating to the CE’s operations. Data aggregation means the combining by a BA of PHI received as a BA of one CE with PHI received as a BA of another CE, to create a collective aggregate database to facilitate and to permit data analyses relating to the health care operations of the respective covered entities, (e.g., contracting with
a quality assurance organization for bench-marking and comparative data reports).

**E. Effective Dates and Transition Period:** CEs must have implemented a BAA with new agreements signed after October 16, 2002 by April 14, 2003. CEs may have operated under existing contracts with BAs for up to one year beyond April 14, 2003, if the contract was not renewed or modified between the effective date of the final rule, October 15, 2002, and April 14, 2003. A CE's contract with a BA will be in compliance with the privacy standard until the sooner of: (1) the date that the contract was renewed or modified after April 14, 2003; or (2) April 14, 2004.

**F. Questions and Communications:** Communication regarding confidentiality and privacy policies and monitoring shall be directed to the Privacy Officer, UCSF Medical Center at 353-1764, or to the UCSF Campus Compliance Office at 476-8642.

**G. Accounting for Disclosures:** Disclosures of PHI for non-permitted uses must be logged and provided to the patient upon request. An Accounting of Disclosures must be provided to a patient at the patient's request. Exceptions to the requirement for an Accounting of Disclosures are listed in UCSF Medical Center Policy 5.02.01, Confidentiality of and Access to Patient Information.

**H. Reporting Violations:** All known or suspected violations of this policy shall be reported to the Privacy Officer or to the Compliance Officer.

**References**

- University of California Business Associate Agreement Templates
- UC Business Associate Amendment (Vendor as BA)
- UC Business Associate Amendment (Reverse Form, UCSF as BA)
- Review Pathway for Business Associate Agreements
- Letter Template: Request for Information from Business Associate
- Letter Template: Determination ? No Business Associate Relationship
- Form Template: Request for Contract Review for BAA
- Form Template: Accounting of Disclosures

---

**Source URL:** [http://policies.ucsf.edu/policy/200-28](http://policies.ucsf.edu/policy/200-28)

**Links:**
[2] mailto:SVCPOLICIES@ucsf.edu