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 but not limited to HIPAA and HITECH. 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 privacy and security laws and regulations 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. This document is not for outside reproduction, distribution or publication without the written permission of The Regents of the University of California.

Definitions

Accounting of Disclosures

A record required to be maintained by the Covered Entity of all disclosures of PHI made to outside entities within the six years prior to the date of a patient's request. This requirement includes disclosures made during a research protocol pursuant to a Committee for Human Research/Institutional Review Board approved Waiver of Authorization. An Accounting of Disclosure must be provided to a patient at the patient's request. Exceptions to the requirement for an Accounting of Disclosures are listed in Medical Center Policy 5.02.01, Confidentiality, Access, Use and Disclosure of PHI and Patient Privacy.

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.

Business Associate Agreement (BAA)

A written contract between a Business Associate and a Covered Entity that specifies the permitted access, uses and disclosures and the safeguards required for PHI by a Business Associate 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 release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

HIPAA


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.

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.

Health Care Provider

Hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for medical services in the normal course of business.

Research Health Information (RHI)

Data used in research that would be personally identifiable but not considered PHI and is therefore not subject to the HIPAA Privacy and Security Rules. The key distinction between RHI and PHI is that PHI is associated with or derived from a healthcare service event, i.e., the provision of care or payment for care. RHI is covered by other state and federal laws for privacy and confidentiality of research health information and human subjects research protections.

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. TPO excludes uses and disclosures of PHI for research.

Use
With respect to individually identifiable health information, 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 Protected Health Information (PHI) may be disclosed to and used by Business Associates as necessary in order to allow the Business Associate to carry out a health care function or activity on behalf of, or to provide services to, UCSF. Business Associates must sign a Business Associate Agreement (BAA) with either the Medical Center, Campus or UC Office of the President (UCOP), 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 Business Associate 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 at 415-353-2750 and shall seek to remedy the breach or, if that is not possible, to terminate the agreement with the Business Associate. Violations by a Business Associate also may be reported by UCSF to the UC HIPAA Compliance Office, the Secretary of the U.S. Department of Health & Human Services (DHHS) and/or the California Department of Public Health (CDPH).

Procedures

Department / Division Responsibility

It is the responsibility of each UCSF department, division or operating unit in collaboration with Procurement and Business Contracts, when contracting for services with outside entities with which PHI will be shared, to ensure that a valid BAA is executed. If it is not clear, whether a contract creates a Business Associate relationship, the contract should be referred to the Director of Procurement and Business Contracts for review.

Responsibilities of the Business Associate

The BAA sets forth the actions for which the Business Associate will be responsible.

Uses of PHI

The Business Associate may not use, access or further disclose the information other than as permitted or required by the BAA and the underlying agreement or required by the contract or as required by law. The Business Associate must limit its use, access, or disclosure, to the extent practicable, to the minimum necessary to accomplish the intended purpose of such use, access, or disclosure.

Security Measures and Safeguards

The Business Associate must use appropriate security measures and safeguards to protect the confidentiality, integrity and availability of PHI from UCSF, and to prevent use, access or disclosure other than as provided in the contract. The Business Associate must maintain written documentation (paper or electronic) of its security measures, update as needed, and make such documentation available to UCSF upon request and in a timely manner.

Reporting, Notification and Corrective Action

The Business Associate must report to UCSF Medical Center any use, access or disclosure of
the information not provided for by its contract of which it becomes aware. The Business Associate must notify UCSF immediately upon discovery of any breach or security incident involving PHI from UCSF.

The Business Associate must take prompt corrective action to remedy any breach or security incident, mitigate any harmful effect of use, access or disclosure of PHI by the Business Associate, and take any other action required by applicable federal and state laws and regulations pertaining to such breach or security incident.

Accounting of Disclosures
The Business Associate must document all disclosures of PHI and make these available to UCSF Medical Center upon written request for an accounting of disclosures.

Patient Access to PHI
The Business Associate must make available to UCSF or a patient, upon request, PHI and any information necessary for UCSF to comply with the patients? rights to access, amend, and receive an accounting of disclosures of their PHI.

Obligations of Subcontractors
The Business Associate must ensure that any subcontractor or agent to whom it provides PHI (either the Business Associate received or created on behalf of UCSF) agrees in writing to the same restrictions and conditions that apply to the Business Associate with respect to the information.

Regulatory Agencies
The BA must make PHI and the BA?s internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health & Human Services (DHHS), the California Department of Public Health, and any other regulatory agency as required by federal and state laws and regulations.

Return or Destroy PHI
At the termination of the contract, the Business Associate must return or destroy all PHI received from, or created or received by the Business Associate on behalf of, UCSF that the Business Associate still maintains in any form. The Business Associate will not retain copies of such information. If such return or destruction is not feasible, the Business Associate will provide UCSF with a written statement of the reason that return or destruction of the information is not feasible, at which point the Business Associate Agreement remains in full force and effect, and further uses or disclosures of the PHI are limited to those purposes that make the return or destruction of the information infeasible.

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 Business Associate. 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 BAA.

This Policy was written in March 2003 and revised in May 2004 and March 2018 to meet HIPAA and HITECH 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 Procurement and Business Contracts Departments, when contracting for services with third parties to whom PHI will be shared, to ensure that a valid BAA is executed prior to the release of any PHI. If it is not clear whether a contract creates a Business Associate relationship, the contract should be referred for review to the Director, Medical Center Materiel Services, or the Campus Purchasing Manager/Associate Director.

B. Exceptions that do not require a BAA:
   1. Disclosures of PHI for treatment, payment or health care operations;
   2. Disclosures of PHI to another Covered Entity, including a health care provider or payer for the payment activities of the entity that receives the information;
   3. Disclosures of PHI to another health care provider for the purpose of treating the patient. Health care providers such as hospitals, physicians, medical groups, etc. are all subject to the Privacy Rule;
   4. Disclosures of PHI to another Covered Entity for health care operation activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is for the detection of fraud and abuse detection or compliance;
   5. Disclosures for financial transactions;
   6. Disclosures between group health plans and plan sponsor;
   7. Disclosures among the CE?s workforce members for TPO;
   8. Disclosures of PHI where any access to PHI would be incidental, if at all, and could not reasonably be prevented;
   9. Disclosures to couriers where the person is a conduit of or carrier for PHI (including both private couriers and their electronic equivalents);
   10. 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;
   11. Disclosures among CEs who participate in an organized health care arrangement (OHCA);
   12. Disclosures of PHI to researchers for research purposes, provided that appropriate consent and Waiver or HIPAA Authorization have been obtained from the patient subjects; and
   13. 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.

C. Exceptions for Data Aggregation Services: Generally, Business Associates are prohibited from using or disclosing PHI in a manner that would be prohibited if used or disclosed by UCSF. However, the BAA may provide that the Business Associate may be permitted to provide data aggregation services relating to UCSF?s health care
operations. Data aggregation means, with respect to PHI created or received by a Business Associate in its capacity as a Business Associate of a Covered Entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the health care operations.

**D. Effective Dates:** Covered Entities must have implemented the 2013 UC BAA template to be in compliance with the HIPAA and HITECH regulations and other applicable laws and regulations.

**E. Questions and Communications:** Communication regarding confidentiality and privacy policies and monitoring shall be directed to the UCSF Privacy Office, at 353-2750, or to the UCSF Campus Compliance Office at 476-1825.

**F. Accounting of 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, Access, Use and Disclosure of Protected Health Information and Privacy.

**G. Reporting Violations:** All known or suspected violations of this policy shall be reported to the Privacy Officer at 353-2750 or to the Compliance Officer at 476-1825.

**References**

- California Health and Safety Code §1280.15 ([6](#ref-6))
- California Civil Code §§1798.82 and 1798.29 ([http://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?tocCode=CIV&division=3.&title=1.8.&part=4.&chapter=&article=](http://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?tocCode=CIV&division=3.&title=1.8.&part=4.&chapter=))
- UC Appendix ? HIPAA Business Associate ([9](#ref-9))
- UCSF Business Associate Agreement template ([10](#ref-10))
- UC Business Associate Amendment (Reverse Template, UCSF as BA): Contact the Privacy Office for the template
- UCSF Supply Chain Management ([11](#ref-11))
- UC HIPAA Business Associates Policy ([12](#ref-12))
- UC Appendix ? Data Security and Privacy ([13](#ref-13))