



University of California
San Francisco

advancing health worldwide™

Advanced HIPAA Institutional Advancement, Communications, and Public Relations

Copyright 2008 The Regents of the University of
California

All Rights Reserved

The Regents of the University of California accepts no liability for any use of this presentation or reliance placed on it, as it is making no representation or warranty, express or implied, as to the accuracy, reliability, or completeness of the presentation.

***HIPAA
Health Insurance Portability and Accountability***

Do I have to take this training?

- ***By law, this training is mandatory for UCSF faculty, staff and volunteers who are involved in:***
 - Communications
 - Fundraising
 - Marketing
 - Media Relations
 - Public Affair
- ***Some members of UCSF's workforce may be required to take additional HIPAA training courses.***

Training Objectives

- ***The purpose of this training is to:***
 - Present a general overview of HIPAA and define important new terms
 - Provide training on the University's specific HIPAA policies
 - Discuss scenarios that illustrate new policies and procedures

- ***Following this training, you will be held responsible for compliance with HIPAA.***

HIPAA is a federal law, and violating it may be a crime.

- ***The University of California, UCSF and UCSF's employees—including volunteers, who are considered an extension of the workforce—face civil and criminal liability.***
 - The University may be exposed to costly lawsuits, and its credibility and reputation will be challenged.
 - You may face penalties of up to \$250,000 and 10 years in jail as well as disciplinary action, including termination.
- ***Now you know why general HIPAA training is required and why specialized training modules—such as this one—have been developed.***

Enforcement of HIPAA as it relates to Institutional Advancement is likely to be complaint-driven.

- ***There are several ways to submit HIPAA complaints. They may be directed:***
 - To UCSF, in which case the Campus will determine what corrective action, if any, is needed
 - To the US Department of Health and Human Services, in which case UCSF may be investigated for HIPAA compliance
 - To an attorney, which could result in costly lawsuits and damage to UCSF's reputation
- ***Understanding the HIPAA regulations will help you avoid activities that are likely to trigger complaints.***

HIPAA—the Health Insurance Portability and Accountability Act—has three main parts:

- ***Privacy Standards—April 2003***
 - Protect an individual’s health information
 - Provide patients with certain rights (e.g., accounting of disclosures)
- ***Security Standards—April 2005***
 - Establish physical, technical and administrative safeguards for electronic transactions
 - Link closely to the Privacy Standards
- ***Codes and Transaction Standards—October 2003***
 - Standardize the way health information is used for claims processing
 - Achieve “administrative simplification” on a national scale

The HIPAA Privacy Standards present some operational challenges, but they also:

- *Reinforce what has always been central to our work—the need to protect patient information*
- *Supplement California’s already strict patient privacy laws*
 - A stricter or more protective rule preempts a less strict or less protective rule.
- *Provide an opportunity to rethink the way we do our work*
- *We have a legal, moral and ethical responsibility to protect patient information as if it were our own.*

HIPAA and the University of California System

- ***UC is a Single Health Care Component.***
 - All 10 UC campuses, UC-managed national labs, etc.
- ***UC has multiple Covered Entities (CEs).***
 - Health Care Providers
 - Medical Centers, Medical Schools, Student Health Services, etc.
 - Self-Insured Health Plans
 - Entities within UC that provide business/financial services to CEs
- ***UC has common policies and procedures for all CEs.***
 - Reduces cost of policy development and implementation
 - Enhances compliance throughout the UC system
 - Minimizes risk

The Key to Compliance: Understand the definition of PHI—Protected Health Information—and when it may be used and disclosed.

- ***PHI is any information related to any individual—including individuals that are not UCSF patients—that:***
 - Is created, received, stored, used and disclosed by the Covered Entity; and
 - Relates to past, present or future physical or mental health; and
 - Describes a disease, diagnosis, procedure, prognosis, condition, payment, etc.; and
 - Exists in any medium—print files, digital files, voicemails, emails, faxes, verbal communications, etc.; and
 - Includes at least one personal identifier of the individual (e.g., name, home and email addresses, fax and phone numbers, SSN, medical record number and other medical identifiers, vehicle identifiers, dates of birth or healthcare service, etc.)

HIPAA tells us that PHI—Protected Health Information—may be used and disclosed for:

- ***Treatment***
 - Broadest permission
- ***Payment***
 - More restrictive permission
- ***Operations***
 - Most restrictive permission
 - Communications, fundraising, marketing, media relations and public affairs fall under Operations.
- ***Certain other uses and disclosures of PHI—such as those required by law—are permitted. But most others will require the patient’s specific authorization.***

HIPAA also tells us how much PHI can be used and disclosed.

- ***The Minimum Necessary Standard applies for all uses and disclosures except for treatment.***
 - Access only what you need to know.
- ***Obtain Authorization when required for:***
 - Fundraising that involves diagnosis or treatment-specific information
 - Disclosures to the media
 - Providing any patient information to a third party for Marketing (as defined in the HIPAA Regulations)
- ***HIPAA permits Incidental Use and Disclosure as long as:***
 - The disclosure is incidental to other permitted uses and disclosures
 - Reasonable safeguards are in place to protect PHI that may be disclosed incidentally
- ***Never use and disclose PHI which you are not allowed to access in the first place.***

UCOP recommends coordination of Institutional Advancement activities with the appropriate campus unit.

- ***This centralized approach is designed to help UCSF:***
 - Assure compliance with HIPAA and other privacy regulations
 - Minimize risk for UCSF and its employees and volunteers
 - Centralize the storage, maintenance and clearance of important HIPAA information
 - Prevent inappropriate or illegal communications, fundraising, marketing, media relations and public affairs activities
- ***Primary points of contact include University Development and Alumni Relations (UDAR), Public Affairs, Medical Center Marketing, etc.***

HIPAA and Fundraising

What do the HIPAA Regulations say?

- ***First the Good News***
 - Fundraising is specifically defined as part of Operations.
 - The Covered Entity may engage in fundraising on its own behalf.
 - The Covered Entity may work with UDAR and the UCSF Foundation as well as UCSF Support Groups and other Business Associates on its fundraising initiatives.
- ***The HIPAA regulations are not trying to put a halt to UCSF's fundraising efforts.***

HIPAA and Fundraising

What do the HIPAA Regulations say?

- ***Some New Operational Mandates***
 - At admission, patients must be given a Notice of Privacy Practices; the Notice must state possible uses and disclosures of PHI, including fundraising, describe the option to authorize disclosures in certain circumstances and list the new rights.
 - An Opt Out mechanism must be included in all fundraising materials.
 - A system to track and honor Opt Out requests must be implemented.
 - Opt Out requests must be maintained for at least 6 years.
 - At UCSF, UDAR shall be the office of record for fundraising Opt Outs.
- ***These new policies and procedures are not optional!***

HIPAA and Fundraising

What do the HIPAA Regulations say?

- ***The Devil is in the Data***
 - The type of PHI that can be used and disclosed for fundraising without Authorization is limited to Demographic Information.
 - Demographic Information is an individual's name, birth date, gender, ethnicity, insurance status, address, dates of service and other contact information.
 - Demographic Information contains no information about the individual's illness or treatment.
- ***Use and disclosure of PHI for fundraising requires an Authorization.***

HIPAA and Fundraising

What do the HIPAA regulations say?

- ***Use and Disclosure of PHI***
 - A signed Authorization must be obtained prior to the use and disclosure of PHI.
 - A member of the patient's Health Care Provider team must initiate the Authorization.
 - If the individual is not a UCSF patient, the development staff or volunteer may initiate the Authorization.
 - The Authorization form must use the HIPAA-prescribed language.
 - At UCSF, UDAR shall be the office of record for fundraising Authorizations.
- ***From a fundraising point of view, unauthorized use and disclosure of PHI is the greatest area of risk.***

Getting Down to Business

Major Gifts and Planned Giving

- ***Health Care Providers may work with UDAR as follows:***
 - A Health Care Provider may provide UDAR with an individual patient's Demographic Information without prior Authorization.
 - A Health Care Provider may provide UDAR with a list of his/her patients and their Demographic Information without prior Authorization as long as PHI is not used to build the list.
 - A Health Care Provider may provide UDAR with PHI only if a signed Authorization is obtained prior to its use and disclosure.
 - In cases where an Authorization is required, a member of the Health Care Provider team should make initial contact with the patient.

Getting Down to Business

Major Gifts and Planned Giving

- ***UDAR may take the lead in fundraising as follows:***
 - UDAR may obtain the name of a patient's Health Care Provider from the Medical Center in order to bring a prospect to his/her attention.
 - UDAR may ask for a list of patients and their Demographic Information from the Medical Center or other Covered Entity without prior Authorization as long as PHI is not used to build the list.
 - UDAR may seek PHI only if a signed Authorization is obtained prior to its use and disclosure.
 - In cases where an Authorization is required, a member of the Health Care Provider team should make initial contact with the patient.

Getting Down to Business Annual Giving and Fundraising Events

- ***How the data is obtained is critical:***
 - Lists for annual giving appeals and fundraising events may be generated using Demographic Information without Authorization.
 - Lists generated using PHI may be used and disclosed only if written Authorizations are on file.
 - Lists may not be refined using PHI as narrowing criteria.
 - Lists—including those that contain Demographic Information only—may not be shared with third-party fundraisers such as the Juvenile Diabetes Foundation without Authorization.
- ***If you don't know how your list was obtained, you don't know if you're in compliance with HIPAA.***

Getting Down to Business

Annual Giving and Fundraising Events

- ***Not all lists will be approved for use:***
 - Discretion should be used to determine the appropriateness of annual giving appeals and fundraising events; this responsibility rests with UDAR.
 - Consideration will be based on legal analysis, data source, planned message, historical precedent and fundraising potential.
 - Lists for all annual giving appeals and fundraising events must be cleared through UDAR.
- ***Ask yourself if annual giving appeals and fundraising events are critical to your program—these are areas of risk.***

Allowing Patients to Opt Out from Fundraising Communications

- ***HIPAA requires that all fundraising communications sent to patients—including invitations to fundraising events—include an easy way for the recipient to Opt Out.***
 - UDAR shall provide standard Opt Out language.
 - UDAR will be the office of record for Opt Out requests.
 - UDAR shall set up systems to track and honor Opt Out requests.
 - UDAR shall approve all printed fundraising materials and lists.
 - Opt Out requests received by Departments, Divisions and other Campus units must be forwarded to UDAR in a timely manner to help assure HIPAA compliance.
- ***Failing to offer, track and/or honor Opt Outs is a clear violation of HIPAA.***

HIPAA and Marketing

What do the HIPAA regulations say?

- ***HIPAA has a unique definition of Marketing. A communication is defined as Marketing when:***
 - It encourages a recipient of the communication to purchase or use a product or service, unless the communication describes a health-related product or service that is provided by the Covered Entity, or;
 - The Campus has received direct or indirect remuneration for disclosure of PHI to a third party to make a communication about its own product or service that encourages the purchase or use of the product or service

Getting Down to Business Marketing

- ***The rules for Marketing are clear and simple:***
 - UCSF cannot provide any information to a third party for purposes that meet the definition of marketing without Authorization.
 - Although HIPAA allows the use of Demographic Information for fundraising purposes, it absolutely prohibits this use for marketing purposes.

Health Care Communication

What do the regulations say?

- ***HIPAA defines many of the things generally considered “marketing” as Health Care Communication. Health Care Communication is defined as when the communication meets one or more of the following criteria:***
 - Occurs in a face-to-face encounter between the patient and health care provider
 - Involves a promotional gift of nominal value
 - Describes health-related products or services that UCSF provides
 - Provides information about the recipient’s treatment or promotes health
in general
- ***An Authorization is not required to use PHI for Health Care Communications.***

Public Affairs

What do the regulations say?

- ***UCOP has determined that Public Affairs is a part of Operations defined in the Regulations as “business management and general administrative activities of the Covered Entity.” Specific activities include:***
 - Providing crisis communications expertise and serving as members of the crisis response team
 - Determining the newsworthiness of stories and other communications that support management and the CE’s operations
 - Collaborating with a patient’s health care provider team in order to protect the patient’s privacy, such as with celebrity patients

Getting Down to Business

Public Affairs

- ***In all circumstances only the minimum necessary information may be used or disclosed.***
 - Requests to physicians or other members of the health care provider team should seek the minimum necessary information to achieve the purpose.
 - Restrict information discussed internally with the physician or other members of the media or health care provider team for purposes of determining the newsworthiness of stories to gender, age, ethnicity, dates of service, city of residence, zip code, occupation and general descriptions of disease or diagnosis.

Getting Down to Business

Public Affairs

- ***In order to provide any PHI to an outside media organization, you must obtain the patient's Authorization using the approved UCSF Authorization form. If you provide general information regarding a patient's disease or treatment protocol you may not provide any of the following identifying information without Authorization:***
 - Name, address (including city and zip code), full face photo or similar images, biometric identifiers (including finger prints)
 - Dates of treatment, date of birth
 - Telephone number, fax number, e-mail address, URL, IP address
 - Social Security number, medical record number, health plan ID number, account number, certificate/license number
 - Device and vehicle identifiers and serial numbers

HIPAA is very specific about how the Authorization is structured.

- ***The Authorization itself must contain very specific language, including but not limited to:***
 - What kind of PHI may be used and disclosed
 - Who can disclose the PHI
 - To whom the PHI will be disclosed
 - For what purpose the PHI will be disclosed
 - When the Authorization will expire
- ***Do not create your own Authorization forms—use only the approved UCSF Authorization forms.***
 - To access the forms, visit the “HIPAA Forms” section of <http://hims.ucsfmedicalcenter.org/>
- ***Note that HIPAA does not recognize verbal authorizations or “negative consent” authorizations.***

HIPAA is very specific about how the Authorization is obtained.

- ***For UCSF patients, the Authorization may be obtained:***
 - By the Health Care Provider, or
 - By a member of the Health Care Provider team, or
 - By a UCSF staff member ONLY if preceded by a conversation between the Health Care Provider and the patient. The Health Care Provider should inform the patient that a staff member will be discussing an Authorization for the purpose of providing his/her information to the media or approaching the individual to discuss fundraising specific to his/her disease or diagnosis
- ***For non-UCSF patients, the Authorization may be obtained:***
 - By a UCSF staff member without prior dialog between the non-UCSF patient and his/her non-UCSF Health Care Provider

HIPAA does not “grandfather” PHI in databases created before April 2003.

- ***Be on the lookout for PHI in the workplace and protect it as if it were your own.***
 - PHI in all formats—FileNet central files, BSR contact reports, personal files, emails, etc.—may not be used or disclosed for fundraising without an Authorization.
 - PHI that is volunteered by a patient about themselves still may *not* be used and disclosed without an Authorization.
 - PHI provided by a volunteer may not be used and disclosed without an Authorization.
- ***PHI obtained after April 2003 is subject to the same policies.***

Understand when a Business Associates Agreement is required.

- ***Vendors or other third parties that use or disclose PHI for or on behalf of the Covered Entity must sign a Business Associates Agreement. Three examples of Business Associates include:***
 - UCSF support groups who may need to use and disclose PHI to generate philanthropic support of UCSF
 - Fundraising consultants working for clinical departments or in any other setting where PHI may be used or disclosed
 - Professional photographers taking photos while on UCSF Medical Center premises
- ***Contact your Purchasing or Business Services manager for assistance with Business Associates Agreements.***

One Last Time

- **H** *Helping UCSF comply with HIPAA is everyone's job.*
- **I** *If you're bending the rules, you may be breaking the law.*
- **P** *Protect PHI as if it were your own.*
- **A** *Always take the most conservative approach.*
- **A** *Ask for permission—with an Authorization—not for forgiveness.*
- *Imagine that it's your PHI, and do the right thing!*

HIPAA Help

• *If you're confused about HIPAA, ask for help! Start with your supervisor or staff contact. You may also get in touch with:*

- **Corinna Kaarlela**
 - Director, News Services
 - 415/476-8254
 - Ckaarlela@pubaff.ucsf.edu
- **Linda Williams**
 - Director, Development Marketing
 - 415/502-5266
 - lwilliams@support.ucsf.edu
- **Mark Gelhaus**
 - Director, Medical Center Marketing
 - 415/353-2716
 - mark.gelhaus@ucsfmedctr.org
- **Deborah Yano-Fong**
 - Chief Privacy Officer
 - 415/353-2750
 - deborah.fong@ucsfmedctr.org
- **Ann Sparkman**
 - Deputy Campus Counsel
 - 415/476-3186
 - asparkman@legal.ucsf.edu

• **UCSF's HIPAA web site at www.hipaa.ucsf.edu/ contains useful HIPAA information.**

Scenario 1

- *The chief of cardiology reports to his assigned development officer that he has just treated the founder of a major San Francisco company and asks the development officer to call the patient and discuss gift opportunities.*
- *Is this a violation of HIPAA?*
- *The cardiologist can provide information about the patient's demographics and dates of service but cannot provide disease-specific information. If the cardiologist would like the development officer to discuss disease-specific information with the patient, the cardiologist should obtain an Authorization first. In either case, the cardiologist should inform the patient that a development officer will be calling.*

Scenario 2

- *The department of surgery asks its assigned development officer to send a fundraising letter to all of its former kidney transplant patients.*
- *Is this a violation of HIPAA?*
- *The department of surgery is asking the development officer to use a fundraising list based on disease-specific information. Neither the department nor the development office may use disease-specific information for fundraising—for direct mail, events or major/planned gifts—without prior Authorization.*

Scenario 3

- ***The Breast Care Center creates a list of breast cancer survivors and subsequently sends this group a Health Care Communication in the form of a newsletter; the newsletter includes a remit envelope for gifts.***
- ***Is this a violation of HIPAA?***
- ***When combining a Health Care Communication with a fundraising appeal, the stricter standard for fundraising applies. In this case, the list is OK for a Health Care Communication, for which PHI may be used without Authorization. However, PHI can be used for fundraising only with prior Authorization. Therefore, a remit envelope for gifts may not be included in the newsletter.***

Scenario 4

- ***The Diabetes Center is asked to provide a list of former patients to the Juvenile Diabetes Foundation (JDF) which, in turn, will solicit the patients for gifts to the JDF.***
- ***Is this a violation of HIPAA?***
- ***The JDF is an outside entity not specifically charged with raising funds for UCSF; as such, it will not qualify for a Business Associates Agreement. Providing PHI of any kind to the JDF is therefore considered marketing and a violation of HIPAA unless the patients have Authorized the disclosure.***

Scenario 5

- *The Children's Hospital has built a new pediatric dialysis facility. It is working with its assigned development officer to invite the families of its diabetic patients to an opening celebration. The cost to attend the event is \$1,000 per person, \$900 of which can be considered a gift.*
- *Is this a violation of HIPAA?*
- *If the invitation is sent to all families of patients of the pediatric dialysis center, this is not a violation of HIPAA. Sending the invitation to a subset of this population would probably require the use of PHI and, thus, would require Authorization. The invitation must include the Opt Out language required by HIPAA for all fundraising communications.*

Scenario 6

- ***UDAR wishes to obtain lists of daily inpatient admissions and review them for known donors as well as prospective new donors.***
- ***Is this a violation of HIPAA?***
- ***Although HIPAA defines fundraising as a part of Operations, UDAR may view only Demographic Information from the Medical Center. UDAR staff may initiate direct contact with a patient only when an Authorization is on file. Alternately, UDAR must work through the Health Care Provider to contact the patient.***

Scenario 7

- ***A fundraising volunteer shares a list of his friends who have had skin cancer with his assigned development officer. They intend to solicit this group for gifts to UCSF's melanoma research program.***
- ***Is this a violation of HIPAA?***
- ***Yes. Members of the UCSF workforce—including volunteers—cannot create, use or disclose PHI that includes disease or treatment specific information for fundraising purposes without Authorization. If a volunteer wants a friend to be contacted by the development officer, s/he should provide name, address and phone number only AND advise the friend that s/he has done so. In other words, volunteers should identify individuals as having “an interest in” a UCSF program and not as having a particular disease.***

Scenario 8

- *The department of neurosurgery needs to purchase an expensive new imaging machine. It plans to ask its neurosurgeons to identify former brain tumor patients and work with UDAR to develop a campaign plan.*
- *Is this a violation of HIPAA?*
- *Yes, unless and Authorization has been obtained from the patient. To access, use and disclose a list of former brain tumor patients for fundraising, a signed Authorization must be on file for each patient. Alternately, the neurosurgeons may generate a list of all their patients—not just those with brain tumors—to be solicited for this project.*

Scenario 9

- ***The thoracic oncology program—which does not have an assigned development officer—pulls a list of its patients (i.e., all former patients of all affiliated physicians) using Demographic Information only and sends out a fundraising letter.***
- ***Is this a violation of HIPAA?***
- ***This is not a violation of HIPAA as long as only Demographic Information is used to pull the list. However, UCSF policy states that all solicitations should be cleared through UDAR. This is critical to assure that all HIPAA requirements—such as honoring existing Opt Outs and providing a mechanism to accept new Opt Outs—have been met.***

Scenario 10

- *A major donor calls UDAR to say that she has a friend who is at the Medical Center for surgery on his back. The donor wants UDAR to ask the CEO to visit her friend.*
- *Is this a violation of HIPAA?*
- *Technically, this is not a violation of HIPAA. However, because the perception could be that UCSF is using a patient's disease information without permission, UDAR should only provide the CEO with the information that the major donor called regarding a friend who is in the hospital. Information regarding the patient's back surgery should not be discussed at this point.*

Scenario 11

- ***A reporter calls Public Affairs asking for the condition of a 43-year old man who was the victim of a car crash. He gives you the patient's name but has no other details. You disclose the patient's condition.***
- ***Is this a violation of HIPAA?***
- ***The Covered Entity may disclose a patient's condition in general terms (good, fair, serious, critical or undetermined) that do not communicate specific medical information as long as the inquiry specifically contains the patient's name and the patient has not placed restriction on release of information. Although California law has permitted hospitals to release a description of the nature of a patient's injuries, this is not permissible under HIPAA without written Authorization.***

Scenario 12

- *A national magazine reporter calls regarding a story on liver transplantations. She would like to interview a patient who has recently undergone a transplant to help illustrate the importance of organ donation. How can the media relations representative find an appropriate patient for the story?*
- *Is this a violation of HIPAA?*
- *A media relations representative may discuss the concept for the story and PHI with a physician to determine if there is an individual who would make a good spokesperson for the institution's liver transplant program. However, the discussion of PHI must be limited to the minimum necessary in order to make the decision and to only those persons who need to know for the decision to be made. Once it has been decided that the patient might be a good spokesperson, the physician should make the initial contact. If the patient agrees, the physician or media relations representative must obtain an Authorization for release of any PHI to the news media.*

Scenario 13

- ***A member of the UCSF staff overhears the name of a well known television personality when it is called out in a patient waiting room. She shares the information with her family at dinner that evening.***
- ***Is this a violation of HIPAA?***
- ***Yes. Although HIPAA tolerates Incidental Use and Disclosure, such as when a name is overheard in a patient waiting room, it does not permit a staff member to discuss that information in any context or setting not directly related to his/her work.***

Scenario 14

- *The department of radiology sends a “negative consent” Authorization letter to its former patients stating that they will assume it is OK to use the patients’ PHI for fundraising unless they request otherwise.*
- *Is this a violation of HIPAA?*
- *Yes. HIPAA does not recognize “negative consent” Authorization, so this is a violation of HIPAA. HIPAA also does not recognize verbal Authorization. Only the approved UCSF Authorization form may be used to obtain permission to use PHI for fundraising.*