



University of California
San Francisco

advancing health worldwide™

Advanced HIPAA Healthcare Provider

Copyright 2008 The Regents of the University of
California

All Rights Reserved

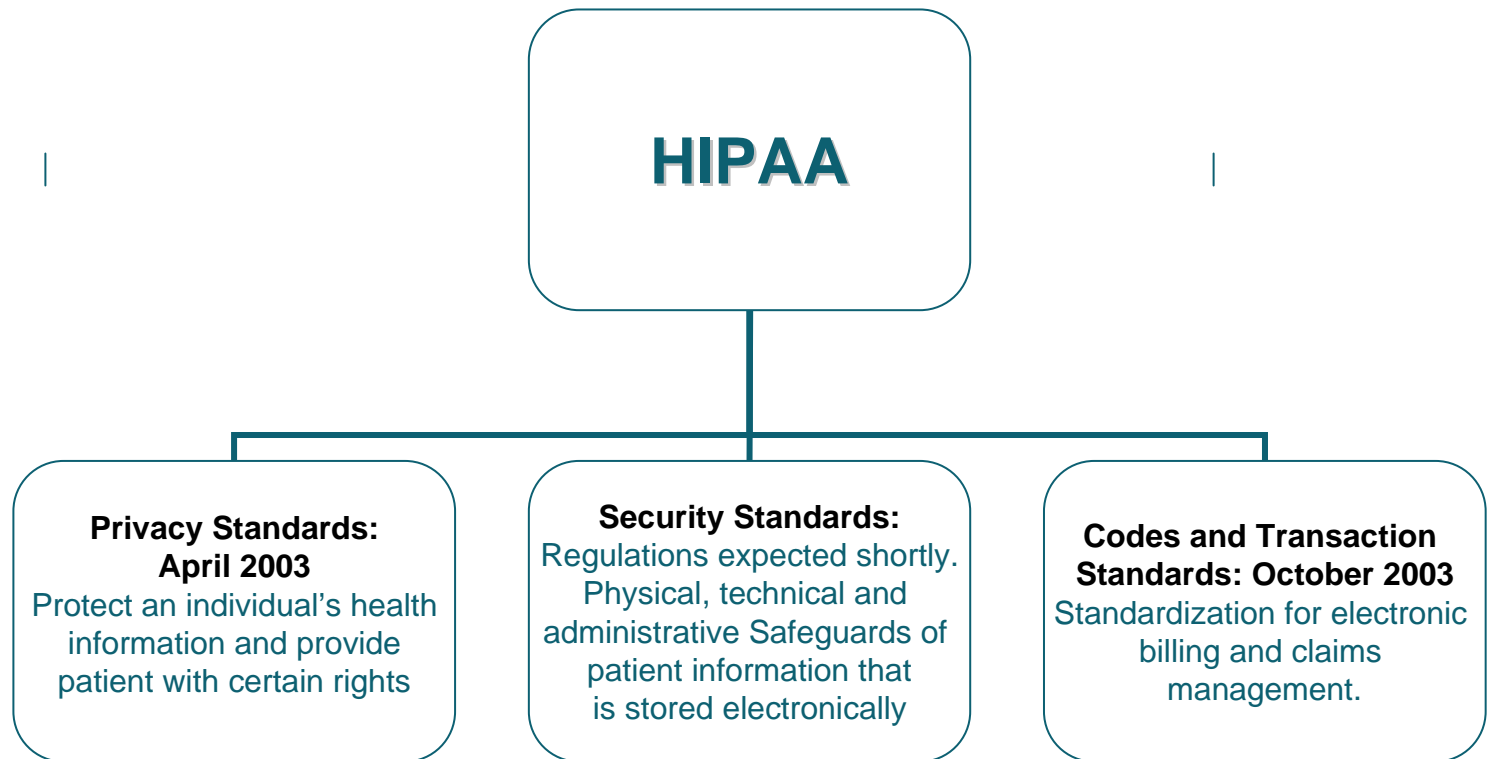
The Regents of the University of California accepts no liability for any use of this presentation or reliance placed on it, as it is making no representation or warranty, express or implied, as to the accuracy, reliability, or completeness of the presentation.

UCSF Healthcare Provider Training Module

Objectives

- Understand what information must be protected under the HIPAA privacy laws
- Understand the HIPAA patient rights
- Understand your role as a healthcare provider in maintaining privacy of protected health information for: patient care, teaching, research, fundraising, marketing and media
- Be aware of consequences for non-compliance

HIPAA, passed in 1996, sought to make health insurance more efficient and portable. Administrative simplification will save the healthcare industry billions of dollars. Because of public concerns about confidentiality, it also addresses information protection.



HIPAA Privacy Standards

- Protect the privacy and security of a person's health information

When

- That health information is used, disclosed or created by a
 - Healthcare Provider
 - Health Plan
 - Healthcare Clearinghouse

What information must you protect?

- Information you create or receive in the course of providing treatment or obtaining payment for services or while engaged in teaching and research activities, including:
 - Information related to the past, present or future physical and/or mental health or condition of an individual
 - Information in ANY medium – whether spoken, written or electronically stored – including videos, photographs and x-rays
- This information is *PROTECTED HEALTH INFORMATION (PHI)*

In order for a UCSF Healthcare Provider to use or disclose PHI

- The University must give each patient a “Notice of Privacy Practices” that:
 - Describes how the University may use and disclose the patient’s protected health information (PHI) and
 - Advises the patient of his/her privacy rights
- The University must attempt to obtain a patient’s signature acknowledging receipt of the Notice, EXCEPT in emergency situations. If a signature is not obtained, the University must document the reason it was not.

The Notice of Privacy Practices allows PHI to be used and disclosed for:

- Treatment
- Payment
- Operations (teaching, medical staff/peer review, legal, auditing, customer service, business management)
- Hospital directories
- Public health and safety reporting
- Other reporting required by government, such as in cases of abuse
- Subpoenas, trials & other legal proceedings

Other uses require authorization

- For many other uses and disclosures of PHI, a written authorization from the patient is needed
 - Example: disclosures to an employer or financial institution or to the media or for research when the IRB has not provided a waiver of authorization
- HIPAA has very specific requirements for the authorization. It must:
 - Describe the PHI to be released
 - Identify who may release the PHI
 - Identify who may receive the PHI
 - Describe the purposes of the disclosure
 - Identify when the authorization expires
 - Be signed by the patient/patient representative

Except for treatment, the “Minimum Necessary” applies

- For patient care and treatment, HIPAA does not impose restrictions on use and disclosures of PHI by health care providers.
 - There are restrictions on disclosure of psychotherapy notes, AIDS test results and substance abuse information.
- For anything else, HIPAA requires users to access the least amount of information necessary to perform their duties.
 - Example: a billing clerk may need to know what laboratory test was done, but not the result.

HIPAA gives patients specific rights

- The right to request restriction of PHI uses and disclosures, such as the use of an alias. Granting restrictions may affect operations, such as the ability to bill for services. Restrictions should not be granted by faculty without consulting the Privacy Officer.
- The right to request alternative forms of communications (mail to P.O. Box not street address; no message on answering machine, etc.).
- The right to access and receive a copy of one's own PHI.
- The right to an accounting of the disclosures of PHI.
- The right to request amendments to information.⁸⁰

Incidental Uses and Disclosures of PHI

- “Incidental” means a use or disclosure that cannot reasonably be prevented, is limited in nature and occurs as a by-product of an otherwise permitted use or disclosure.
 - Example: discussions during teaching rounds; calling out a patient’s name in the waiting room; sign in sheets in hospital and clinics.
- Incidental uses and disclosures are permitted, so long as reasonable safeguards are used to protect PHI and minimum necessary standards are applied.
- **HELP KEEP PHI CONFIDENTIAL**

Consider the following example:

1. You are a healthcare provider. Your friend's spouse is in the hospital after an accident. Your friend asks you to review what treatment has been provided to the spouse and see if you concur. What are you able to do under HIPAA?
 - A. Access the person's chart so that you can communicate with your friend about the patient's condition.
 - B. Contact the charge nurse on the floor and ask her to look into the patient records for you.
 - C. Advise your friend that you can only look at the medical records if you are treating the patient or you receive the patient's authorization to review the medical record.

Answer:

- C. Under HIPAA you are only allowed to use information required to do your job.

Since you are not part of the patient care team, it is against the law to access the patient record or ask someone to access it on your behalf – even though you may know the person and just want to be helpful. Remember, that if you were in a similar situation, you may not want your colleagues going through your medical records or those of your spouse or close friend.

Consider the following example:

2. The father and mother of an adult married competent patient are visiting the patient. As a member of the care team, you need to review and provide education to her on the new meds ordered by the physician. One medication is Prozac, a well known anti-depressant. What is the best way to approach a patient when her relatives are in the room?
 - A. Ask the patient's relatives to leave the room.
 - B. Go ahead and explain the medications to her. She won't mind her family members overhearing.
 - C. Explain to the patient that you need to discuss her medications with her, and that the information is confidential. If she says her relatives may stay in the room, go ahead explain the medications to her.

Answer:

- C. Never assume that the patient has shared her medical information with her relatives.

You should ideally ask the patient's relatives to step out of the room. If the patient understands that the information is sensitive and she agrees to have her relatives present, you can go ahead and have the discussion with the patient.

The answer would be the same if it had been her husband visiting her. The patient may not have shared all of the information with her husband.

Penalties for Violations

- A violation of federal regulations or University Policy can result in discipline, loss of employment, fines or imprisonment.
- If a disclosure of PHI is made willfully and with an intent for personal gain, the penalty can be as high as a \$250,000 fine and 10-year imprisonment. The University would not consider such an action as in the course and scope of your employment and would not defend you.

Use or disclosure of psychotherapy notes to a third party requires the patient's Authorization except:

- Use by the originator of the notes for treatment purposes;
- Use or disclosure by UC for its own mental health training programs;
- Use or disclosure by UC to defend itself in a legal action or other proceeding brought by the individual;
- Use or disclosure that is required or permitted with respect to oversight of the originator of the notes.

Mental health PHI disclosures to the individual

- Unlike HIPAA, California Law allows the individual access to his/her mental health PHI, including psychotherapy notes, upon the patient's written request
- UC can deny access to mental health PHI if there is a substantial risk of physical harm/ endangerment of life to the patient, in the professional judgment of the provider

How does HIPAA affect teaching activities?

- Allows the use and disclosure of PHI for the teaching of University of California students (all health professions programs).
- Allows the exchange of PHI for teaching purposes between UCSF and other covered entities, so long as both institutions have a teaching relationship with the patient .
- HIPAA does not allow the use and disclosure of PHI to individuals who do not have a teaching relationship to the University or a teaching relationship to the individual (e.g., attendees at CME conferences or medical/health professions' lectures). **USE DE-IDENTIFIED INFORMATION OR OBTAIN AUTHORIZATION.**

Limited Data Set removes Direct Identifiers from PHI

- Facial identifiers
- Medical record numbers
- Health plan beneficiary numbers
- Device identifiers and serial numbers
- Biometric identifiers
- With the removal of the Direct Identifiers, the data may be used and disclosed if a Data Use Agreement is in place (e.g., between UCSF and the PHI recipient)
- See the Privacy Officer, Campus Counsel or HIMS Department for assistance with the Data Use Agreement

HIPAA allows the use of a Limited Data Set for Teaching, Research & Public Health

- Allied health professionals from a non-covered entity
- CME and other Education to individuals or entities who may not be part of UC
- Teaching material for undergraduate education
- Research purposes

Uses and Disclosures of PHI for Research

- In order to access or use PHI or databases maintained by a UC health care provider or medical center for research purposes, the researcher must obtain appropriate IRB approval of the research protocol.
- Additional education on HIPAA research requirements will be provided to investigators and UC health care providers who also engage in research.

PHI Research Restrictions Go Beyond Clinical Trials

- In addition to human subjects in clinical trials, PHI can also be associated with the use of specimens and data from humans:
 - Medical Records Review (both living and deceased subjects)
 - Biological specimens (tissue, urine, saliva)
 - Biometrics (images audios, videos, fingerprints)
 - Data sets (depending on type of identifiers attached)
 - Recruitment of potential subjects for research from PHI sources (medical records, databases, etc)

What if a research investigator wants information about my patients?

- Treating physicians cannot discuss their patients and their PHI with research investigators for the purpose of recruitment. However, providers can inform their patients about research studies. For example:
 - Research investigators can inform providers that there are research studies and clinical trials available to subjects (examples: by information letter, flyers, website, brochures)
 - Treating physicians can inform their patients of research studies that the patients might be interested in
 - Patients can contact the research studies they heard about from their treating physicians or from advertisements, flyers

How does a researcher gain access to PHI from medical records?

- Health Information Management Services will require the investigator to show one of the following as proof of authorization to view PHI:
 - Copy of CHR Approval Letter with statement of Waiver of Consent/Authorization of individual consent to access PHI
 - Copy of CHR Approval Letter with statement that individual subject consent/authorization will be obtained to access PHI
 - Copy of Individual Authorization signed by research subject

Uses and Disclosures of PHI by Fundraising Staff

- May only use demographic information and dates of service for fundraising. Disease, diagnosis or condition may not be used to develop a fundraising mailing list.
- Must obtain a patient's authorization to use any other PHI for fundraising.
- Faculty may provide the Development Office with a list of individuals who can receive a fundraising solicitation or can send fundraising solicitations to a list that they have created using their own patients' demographics.
- All fundraising material must provide the recipient with a way to opt out of receiving any additional fundraising material.
- All fundraising efforts must be coordinated with the UCSF Development Office.

Uses and Disclosures of PHI for Marketing

- A UC health care provider may use PHI to communicate to the patient about:
 - a product or service UC provides
 - general health issues: disease prevention; wellness classes, etc.
- For all other marketing, particularly when a third party requests access to a faculty's patient list for purposes of marketing a product, a patient authorization must be obtained
 - The Authorization must state whether UC has received any direct or indirect remuneration for providing the list or other PHI
- Any questions should be directed to the UCSF Marketing Department, to the Office of the General Counsel or to the UC HIPAA Privacy Officer

Consider the following example:

3. A physician is invited by a drug company rep to play golf. During the game, the rep begins talking about a new COX-2 inhibitor the drug company is developing. The physician gives the rep names and phone numbers of a few patients with arthritis, believing that they could benefit from the new treatment. A week later, the patients call the doctor's office complaining about being solicited by the drug company to take part in a clinical trial. What does HIPAA say about this?
 - A. Since the physician had good intentions, the physician has not violated HIPAA.
 - B. Physicians should stop associating with drug company reps as there are many circumstances that could result in violations of federal law, including HIPAA.
 - C. Since PHI was disclosed for purposes other than what state and federal law allows, an authorization from the patients should have been obtained before the PHI was released.

Answer:

- C. This is an example of marketing under HIPAA. PHI was IMPROPERLY disclosed.

Never provide information to a friend, colleague or business representative UNLESS it is required as part of your job and permitted under HIPAA and/or other state and federal laws. Always keep your patient's information confidential to maintain your rapport and the patient's trust. Providing an unauthorized release of information to a drug rep for marketing or research purposes violates state and federal law. This could be interpreted as an illegal disclosure for personal gain (the value of the round of golf) and subject you to a hefty fine and imprisonment.

Uses and Disclosures for Communications with the Media

- The patient's healthcare provider must be the initial contact with the patient for communication with the media or for developing University communications that use PHI.

And

- The healthcare provider must obtain the patient's authorization for the use and disclosure to the media.

HIPAA Do's and Don'ts

- Treat all patient information as if you were the patient. Don't be careless or negligent with PHI in any form, whether spoken, written or electronically stored.
- Shred or properly dispose of all documents containing PHI that are not part of the official medical record. Do not take the medical record off of University property. Limit the PHI you take home with you.
- Use automatic locks on laptop computers and PDAs and log off after each time you use a computer. Do not share passwords. Purge PHI from devices as soon as possible.

HIPAA Do's and Don'ts

- Use secure networks for e-mails with PHI and add a confidentiality disclaimer to the footer of such e-mails. Do not share passwords.
- Set a protocol to provide for confidential sending and receipt of faxes that contain PHI and other confidential information.
- Discuss PHI in secure environments, or in a low voice so that others do not overhear the discussion.

Consider the following example:

4. A physician and a nurse were discussing a patient in an elevator filled with people. In the conversation the patient's name, diagnosis and prognosis are mentioned. What could have been done differently to protect the patient's privacy?
 - A. The patient's privacy was protected, nothing was done wrong since no written PHI was exchanged.
 - B. It is important to be aware of your surroundings when you discuss patient information (PHI). The patient's case should have been discussed in another room, away from other patients, or at least in low voices that could not be overheard.
 - C. No patients or patient families should be allowed to use hospital staff elevators to avoid such situations.

Answer:

- B. Although HIPAA allows incidental uses and disclosures, this type of disclosure is not allowed. PHI includes oral communications. The patient's case should have been discussed in a location that allowed for privacy of the information discussed.

Consider the following example:

5. As a resident downloads a patient file into her PDA, a code blue is called. In her hurry to respond, she leaves her PDA in its cradle. When she returns, the PDA is gone. What does HIPAA require?
 - A. HIPAA says nothing because a copy of a patient's file on a PDA is not PHI.
 - B. The resident has a responsibility to make certain that her laptop, PDAs, and other equipment are password protected and have an automatic key lock.
 - C. HIPAA does not allow the use of PDAs to store PHI.

Answer:

- B. HIPAA requires that everyone protect PHI, whether in electronic, oral or written form. Using passwords and automatic key locks provides for the security of PHI since anyone without the password cannot access the files.

Consider the following example:

5. You are in the ER examining a 6-year-old boy and observe cigarette burns on the arms and hands of the boy. What does HIPAA require you to do?
 - A. HIPAA requires you to protect patient confidentiality so no disclosure of PHI should be made.
 - B. Patient safety is involved, and federal and state law require that you report this.
 - C. HIPAA does not allow you to report this incident, but state law requires it.

Answer:

- B.** While HIPAA requires you to maintain patient confidentiality, exceptions exist which allow PHI disclosures. State law requires and HIPAA allows the reporting of child or elderly abuse and communicable diseases.

Remember:

- PHI is contained in the designated record set. Should you copy any protected information for your use to a PDA, 3x5 card, slip of paper or other site – it is your responsibility to safe guard and destroy it once it is no longer needed.
- It is everyone's responsibility to protect PHI and you may be at personal financial risk if you fail to do so.

Thank you!

- Help us to improve privacy / security of protected health information (PHI).
- Report improper disclosures of PHI so UCSF can meet its obligation to mitigate consequences.
- Report privacy concerns to the Compliance Office, hot line (415) 502-8448, or Privacy Office.
- Contact UCSF Privacy Office at 353-2750 for more information on HIPAA or visit our website:

<http://hipaa.ucsf.edu>

HIPAA Resources

- HIPAA Handbook
- HIPAA 101 - Basic Training Module
- General HIPAA information
<http://hipaa.ucsf.edu>
- UCSF Medical Center IT
<http://it.ucsfmedicalcenter.org/>
- UCSF Information Security
<http://security.ucsf.edu/>