HIPAA
Health Insurance Portability and Accountability Act

- *Education Module for Institutional Advancement, Communications and Media Relations*

Training Objectives

- 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 and the University of California System

- *The Regents have designated UC as a Single Health Care Component with many entities covered by HIPAA (CEs)*
  - Health Care Providers (individuals & entities) at all campuses and federal Department of Energy Labs
  - Medical Centers, Medical Schools, Student Health Services, etc.
  - Self-Insured Health Plans
  - Entities within UC that provide business/financial services to CEs
- *The UC Single Health Care Component's HIPAA Taskforce has developed common policies and procedures for all CEs.*
  - Reduce cost of policy development and implementation
  - Enhance compliance throughout the UC system
  - Minimize risk

HIPAA has three main parts:

- *Privacy Standards—April 2003*
  - Protect an individual's health information
  - Provide patients with certain privacy rights
- *Security Standards—April 2005*
  - Establish physical, technical and administrative safeguards for electronic transactions
  - Link closely to Privacy Standards
- *Codes and Transaction Standards—October 2003*
  - Achieve "administrative simplification" on a national scale to provide savings and facilitate payments

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

- *The UC Single Health Care Component (SHCC) and its employees 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, for deliberate violations of HIPAA and UC policy.

Now you know why general HIPAA training is required and why specialized training modules—such as this one—have been developed.

Enforcement of HIPAA is likely to be a complaint-driven process.

- Complaints may be directed to each campus Privacy Officer or Liaison or to the University's Privacy Official.
- Complaints may be directed to the US Department of Health and Human Services
- Complaints may be directed to an individual's attorney.

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

- *Reinforce what has always been central to our work—the need to protect patient information*
- *Supplement California's already strict patient privacy laws*
- *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.

Understand the definition of PHI and when it can be used or disclosed.

- *PHI is any information related to a SHCC patient that:*
  - Is created, received, stored, used and disclosed by the Covered Entity (CE); 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 of the personal identifiers of the individual, the individual's family or household member or employer (e.g., name, home and email addresses, fax and phone numbers, Social Security number, medical records and other medical identifiers, vehicle identifiers, dates of birth or healthcare service, etc.)

PHI—Protected Health Information—may be used and disclosed for:

- *Treatment*
  - Broadest permission
- *Payment*
  - More restrictive permission
- *Operations*
  - Most restrictive permission
  - Fundraising and media fall into this category.
- *Certain other uses and disclosures of PHI—such as those required by law—are also 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 treatment*
  - Access only what you need to know and no more
- *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
- *HIPAA permits incidental use and disclosure as long as:*
  - Reasonable safeguards are in place
  - The PHI is not subsequently used or disclosed in violation of the Regulations

Some new operational mandates

- At admission, patients must be given a Notice of Privacy Practices which describes possible uses and disclosures of PHI, including fundraising
- Patients have the right to exercise a number of new privacy rights and to Authorize disclosures for certain activities
- The CE must document that it has met certain mandates
- An Opt Out mechanism must be included in all fundraising materials; a system to track and honor Opt Out requests must be implemented and maintained for six years

These new policies and procedures are not optional!

Responsibility for coordinating fundraising, media and community relations

- *All fundraising activities and questions relative to media and community relations activities should be coordinated with the local responsible office and individuals*
  - Assures compliance with HIPAA and other regulations
  - Prevents inappropriate or illegal fundraising, media or community relations activities
  - Minimizes risk for the University and its employees
  - Maximizes fundraising potential

HIPAA and Fundraising
What do the HIPAA Regulations say?

- *First the Good News*
  - Fundraising is specifically defined as part of Health Care Operations.
  - The CE may engage in fundraising on its own behalf.
  - The CE may work with the Development Office and institutionally related foundations and/or business associates on its fundraising initiatives.
    - Foundation members who use a patient's demographic information for fundraising purposes must be trained on HIPAA or, if not part of the SHCC workforce, enter into a Business Associate Agreement with the campus.

The HIPAA regulations are not trying to put a halt to fundraising efforts.

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 Non-Demographic PHI Requires Authorization

- A signed Authorization must be obtained prior to the use and disclosure of non-Demographic PHI.
- A member of the patient's Health Care Provider team must initiate the Authorization.
- UC has developed an Authorization form that meets all HIPAA-required language
- Contact the Development Office or Privacy Officer for the required Authorization Form
- _____is 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.

Major Gifts and Planned Giving

- *Members of the Health Care Provider Team may work with the Development Office as follows:*
  - A Health Care Provider may provide an individual patient's Demographic Information without prior Authorization.
  - A Health Care Provider may provide a list of his/her patients and their Demographic Information without prior Authorization so long as PHI is not used to build the list.
  - A Health Care Provider may provide PHI (including disease or treatment information) only if a signed Authorization is obtained prior to its use by the Development Office.
  - In the case where an Authorization is required, a member of the Health Care Provider team should make initial contact with the patient.

The Development Office may take the lead in fundraising:

- Obtain the name of a patient's Health Care Provider from the Medical Center in order to bring a major prospect to the provider's attention.
- Obtain a list of patients and their Demographic Information from the Medical Center or Covered Entity without prior Authorization so long as the list is built based on dates of service or other non-disease or treatment information
  - The Development Office may not ask medical records or other data managers to provide demographic information for a list of patients if PHI were used to build the list.
- Use PHI only if a signed Authorization is obtained prior to its use and disclosure.
- In the case where an Authorization is required, a member of the Health Care Provider team should make initial contact with the patient.

How the data is obtained is critical

- Lists for annual giving appeals and fundraising events may be generated using Demographic Information only.
- 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.

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 the Development Office
- 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 _____

Ask yourself if annual giving appeals and fundraising events are critical to your program—

these are areas of risk.

Allowing Patients to Opt Out

- *HIPAA requires that all fundraising materials that target patients—including event invitations—include an easy way for the recipient to Opt Out.*
  - _____ will be the office of record for Opt Out requests.
  - _____ shall provide standard Opt Out language.
  - _____ shall approve all printed materials before they go to press.
  - _____ shall set up systems to track and Opt Out requests.

Failing to offer, track and/or honor Opt Outs is a clear violation of HIPAA.

What does HIPAA say about 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 CE; or
  - The Campus has received direct or indirect remuneration for disclosure of PHI to a third party for the third party to make a communication about its own product or service that encourages the purchase or use of the product or service.
  - Faculty, members of the provider team and others within the CE cannot provide any information to a third party for purposes of marketing activities without the patient's Authorization
  - Although HIPAA allows the use of demographics, including patient name and address, for fundraising purposes, it absolutely prohibits providing a list of patients and their demographics to outside parties for marketing purposes

Health Care Communications are not marketing under HIPAA

- HIPAA defines many of the things generally considered "marketing" as Health Care Communications. The following are considered Health Care Communications:

  - Occurs in a face-to-face encounter between provider or CE and patient;
  - Involves a promotional gift of nominal value;
  - Describes health-related products or services that the CE or UC covered individual provides; or
  - Provides information about the recipient's treatment or promotes health in general

No Authorization is required for these activities

Community and Public Affairs, Media Relations

- HIPAA does not define “media and community relations” or provide specific guidance regarding these activities (although there are specific requirements for fundraising and marketing)
- UC has determined that public affairs, community and media relations are a part of operations under the operations activity of “business management and general administrative activities of the entity” and 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 entity’s operations
  - Participating on the patient care team in order to protect the patient’s privacy, including celebrities

Community and Public Affairs, Media Relations

- However, in all circumstances only the **minimum necessary** information can be used by members of the workforce to carry out these activities
  - **Limit requests** to physicians or other providers to the minimum necessary to achieve the purpose
  - In general, restrict information **discussed internally** with the physician or other members of the media or provider team for purposes of determining the newsworthiness of stories to:
    - Gender, age, ethnicity, dates of admission or discharge, city of residence (by zipcode), occupation and general disease or diagnostic health information

Obtain a patient-signed Authorization to disclose PHI to the media

- In order to provide ANY PHI to an outside media organization, you must obtain the patient's Authorization using the UC approved HIPAA Authorization form
- If you provide general information regarding the individual's disease or treatment protocol you may not provide any patient identifying information, including one or more of the following, unless you have Authorization
  - Name, Address including city and zip code, Full face photo and other comparable image, Biometric identifier 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 number

Conclusion: HIPAA requires an Authorization for all the following

- Fundraising activities that use disease or treatment information—i.e., more than demographic information
  - Including building a fundraising list or inviting a select group of individuals to an event if the invitation is based on the individual's diagnosis or treatment protocol
- Marketing activities of any type, including providing only a list of patient names to outside entities or third parties
- Media and community relations that use any type of PHI

HIPAA-specific Authorization

- *The Authorization itself must contain very specific language, including but not limited to:*
  - Exactly what kind of PHI may be used and disclosed
  - The purpose of the disclosure
  - Who can disclose the PHI
  - To whom the PHI will be disclosed
  - When the Authorization will expire

Do not try to create your own Authorization forms—use ONLY the approved UC Authorization form.

HIPAA does not recognize verbal authorizations or "negative consent" authorizations.

HIPAA is very specific about how the Authorization is obtained.

- *The Authorization may be obtained:*
  - By the Health Care Provider
  - By a member of the Health Care Provider team
  - By a Development, Media or Community Relations staff member if preceded by a conversation between the Health Care Provider and the patient. The 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 diagnosis or treatment

It is strongly recommended that the Health Care Provider/patient conversation be documented when staff will be obtaining the Authorization.

HIPAA does not "grandfather" PHI data bases 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 (if it is the patient's PHI) may be used and disclosed; it is strongly recommended that the time and place the disclosure was made be documented.
  - When a volunteer or member of the workforce offers to provide you with a list of names that includes diagnosis or treatment, carefully consider the source of the information, always use discretion in using such information, and determine whether the use of this PHI for targeted solicitations could put you or UC at risk

PHI obtained after April 2003 is subject to the same policies.

Business Associates

- HIPAA allows a CE to disclose PHI to a third party contractor or vendor for certain activities, including fundraising, so long as there is a Business Associate Agreement between the CE and the Business Associate
- If an Authorization is required, you must also obtain an Authorization for uses and disclosures by a Business Associate
- Seek advice from the Privacy Officer, Procurement or Materiels Manager or General Counsel

Let common sense—and an understanding of the law—be your guide.

- Know when and how to use PHI, and obey the Minimum Necessary Standard.
- Avoid sending PHI in unsecured email, fax or other communications; use confidentiality statements in the footer.
- Do not share PHI with anyone unless they are permitted by HIPAA or other law to receive PHI
- Never enable others to access PHI by leaving files unattended, sharing your passwords, etc.
- Report possible HIPAA violations to your supervisor immediately. HIPAA requires the CE mitigate the impact of any violations—accidental or deliberate

Imagine that it's your PHI...

and do the right thing!

One Last Time

- H *Helping UC 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—through an Authorization--not for forgiveness.*

HIPAA Resources and Help

- If you're confused about HIPAA, ask for help!
- University Privacy Officer—maria.faer@ucop.edu
- Campus Privacy Official or General Counsel
- Your supervisor
- University's HIPAA web-site includes:
  - Notice of Privacy Practices
  - University's Systemwide Standards and Implementation Policies
  - Authorization Form (s)
  - Business Associate Agreement
  - Other Education Modules

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 health care provider can provide information about the patient's demographics and dates of service to the development officer, but can not provide specific disease or treatment information. If the cardiologist would like the development officer to discuss specific treatment information with the patient, the provider must obtain the patient's authorization to be contacted by the development officer.

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 create a fundraising list and solicitation based on disease and treatment specific information. The development officer is not allowed to use disease specific information unless the provider has obtained Authorization from the kidney transplant patients for fundraising purposes or the medical center has obtained the patient's authorization at admission or discharge to be contacted by the University's development officer.

Scenario 3

- The Breast Care Center uses PHI to pull a list of breast cancer patients 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?

- The Breast Care Center treats a broad range of patients, including those with breast cancer. The Center cannot create a fundraising/development list of patients that is disease specific without patient Authorization, even if it is inserted into a Health Care Communication. The Health Care Communication is allowed under HIPAA, but the fact that it includes a targeted fundraising solicitation is a violation. The Development office should send the Health Care Communication as a standalone newsletter. The targeted fundraising campaign must be done with patient Authorization.

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 the campus; as such, it will not qualify for a Business Associates Agreement. Providing a patient list of any kind—regardless of whether or not the data contains Demographic or non-Demographic information—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 you have sent an invitation to all families of patients at the dialysis center, you can do this, but you must include the opt out language required by HIPAA as a part of the invitation.

Scenario 6

- The Development Office wants to obtain lists of daily inpatient admissions and review them for prospective donors.

  Is this a violation of HIPAA?

- As a part of healthcare operations, the Development Office may view only demographic information from the Medical Center and may initiate direct contact with a patient only when an Authorization is on file. Alternately, the Development Office must work through the health care provider team to contact the patient.

Scenario 7

- A campaign 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 the medical center's melanoma research program.

  Is this a violation of HIPAA?

- This raises several issues. First, the volunteer is a part of the CE's workforce (otherwise, they would have to be considered a Business Associate) and is subject to the same requirements as any other member of the workforce, including a physician. The volunteer has created a disease specific list or PHI. Some of the names may be those of the medical center's former patients. Under HIPAA, a member of the CE's workforce cannot create, use or disclose PHI that includes disease or treatment specific information for fundraising purposes, without Authorization. If a volunteer wants his friend to be contacted by the development officer, he should only provide the name, address and phone number AND advise the friend that he has done so. The Development Office could also send an invitation that references the campaign volunteer in the mailing.

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 the Development Office to develop a campaign plan.

  Is this a violation of HIPAA?

- Yes, unless an Authorization has been obtained by the provider from the former patients. Again, Authorization from the patient could have been obtained upon discharge or admission to be contacted by the development office. 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

- A clinical division with no assigned development officer pulls a list of its patients using Demographic Information only and sends out a fundraising letter.

  Is this a violation of HIPAA?

- No, but UC policy is that providers and departments should contact the Development Office prior to sending out a fundraising letter to assure that all HIPAA requirements have been met—e.g., to include specific opt out language and to provide a mechanism for tracking opt outs.

Scenario 10

- A Development Office staff member working on the Cancer Center campaign logs on to FileNet because s/he wants to try to substantiate a tabloid story that a former UC patient who is also a celebrity (and a major donor to the AIDS Research Institute) has AIDS. S/he finds PHI, along with a signed Authorization for fundraising, in FileNet and shares the story with her family that evening.

Is this a violation of HIPAA?

- Yes, potentially 3 violations: 1) The medical center should have established a mechanism for preventing access to FileNet by the development office if that database includes disease specific information and it was not role-based access; 2) Unwarranted access to more information than necessary by the staff member who has been trained that she cannot access disease specific information without Authorization; 3) disclosure by the staff member to a family member.

Scenario 11

- A major donor calls the Development Officer saying that she has a friend who is at the Medical Center for surgery on his back. The donor wants the Development Officer to ask the Dean or Hospital Director to visit her friend.

Is this a violation of HIPAA?

- Again, because the perception could be that UC is using a patient's disease information without permission, the Development Officer should only provide the Dean or Hospital Director with information that the donor had called regarding a friend who is in the hospital. Information regarding the patient's back surgery should not be discussed by the Development Officer. When the Dean or Director visits the patient, then that information may be provided by the patient.

Scenario 12

- A reporter calls 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. What information can you release to the reporter?

- Covered entities 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 13

- 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?

- 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.

Conclusion:

Privacy of health information is everyone's right and everyone's responsibility.

Thank you for doing your part in protecting our patient's information.