UCR | School of Medicine
UCR Health

Compliance & Privacy Program

HIPAA For Institutional Advancement

UNIVERSITY OF CALIFORNIA, RIVERSIDE

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) which includes the Medical Center, Ambulatory practices, and the School of Medicine, as well as entities within UC that provide business/financial services to Ces.

The University has developed common policies and procedures for all components of the covered entity including a UC Fundraising policy which was last updated in July 2010

Training Objectives

At the conclusion of this training, you should be able to:

- Present a general overview of HIPAA and define important terms.
- Know what’s changed since 2003.
- Know what’s changed by the HIPAA Omnibus Rule of 2013.
- Provide training on the University’s fundraising-specific HIPAA policies.
- Discuss scenarios that illustrate the policies and procedures.

What is Protected Health Information (PHI) and When Can it be Used and Disclosed?

PHI is any personally identifiable information related to a patient that:

- Is created, received, stored, used and disclosed by the Covered Entity
- Relates to past, present or future physical or mental health
- Describes a disease, diagnosis, procedure, prognosis, condition, payment, etc.
- Exists in any medium—print files, digital files, voicemails, emails, faxes, verbal communications, etc.

HIPAA and Fundraising – What Do The HIPAA Regulations Say?

First, the Good News!

Fundraising is specifically defined as part of Health Care Operations!	The Covered Entity may engage in fundraising on its own behalf!
The Covered Entity 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 information for fundraising purposes must be trained on HIPAA or, if not part of the Single Health Care Component (SHCC) workforce, enter into a Business Associate Agreement with the campus!

HIPAA and Fundraising – What Do The HIPAA Regulations Say?

The Devil is in the Data!

Until the passage of the new HIPAA Omnibus Rule, the only type of PHI that could be used and disclosed for fundraising without Authorization was limited to demographic information and dates of service.

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.

HIPAA and Fundraising – What Do The HIPAA Regulations Say?

The Devil is in the Data!

The HIPAA Omnibus Rule, effective September 23, 2013, added categories that may be used or disclosed for fundraising, as follows:

- Academic Department or Service
- Treating Physician
- Outcome Information
- Health Insurance Status

Example: A physician desiring to raise funds for a new cancer center may concentrate its efforts on oncology patients who have had positive outcomes and are not uninsured.

All other use and disclosure of PHI for fundraising requires an Authorization.

Use and Disclosure of PHI Not Specifically Allowed Requires Authorization

A signed Authorization must be obtained prior to the use and disclosure of PHI not specifically allowed by the HIPAA Omnibus Rule

A member of the patient's Health Care Provider team must initiate the Authorization

University Advancement has developed an Authorization form that meets all HIPAA-required language

University Advancement (UA) is the office of record for fundraising Authorizations

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 the allowed individual patient Information without prior Authorization.

- 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 a list of patients and their allowed Information from the Ambulatory Practices 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 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.

How the Data is Obtained is Critical

- Lists for annual giving appeals and fundraising events may be generated using allowed information only.
- Lists may not be refined using PHI as narrowing criteria.
- Lists—including those that contain allowed 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 UA.

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 University Advancement.

Opt Out

HIPAA requires that all fundraising materials provide an easy way for the recipient to Opt Out. *The new HIPAA Omnibus Rule requires that the opportunity to "opt out" be "clear and conspicuous", that the method for opting out not require an undue burden and that the covered entity discontinue fundraising communications after the individual has opted out.*

Opt Out

- Office of Development will be the office of record for Opt Out requests and shall provide standard Opt Out language.
- Office of Development shall approve all printed materials before they go to press.
- University Advancement shall set up systems to track ‘Opt Out’ requests and provide an individual who has opted out with a method to opt back in to future fundraising communications.

Failing to offer, track and/or honor Opt Outs is a clear violation of HIPAA. Regulations are also proposed that a “good faith” effort to track opt outs will not be enough. A patient opt out will be considered a revocation of authorization

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 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*.*

Enforcement Changes

The UC Single Health Care Component (SHCC) and its employees may face civil and criminal liability for privacy breaches.

- Enforcement has increased since 2003 and there are additional challenges with electronic information.
- There is mandatory reporting of breaches both at the State level and federal level with significant fines for the university and possibly for the individual, as well.

Privacy and Security Basics

- Become familiar with the UCR Health Privacy & Security Policies. These are on the UCR Health intranet website. Key policies include fundraising, encryption of data on portable devices, social media, and use of PHI in email.

- Email: If sending PHI outside of UCR Health or even within, use encrypted email ("Send Secure").

- PHI that is maintained locally on a laptop, computer, or other devices, such as flash drives, must be encrypted. New laptops purchased by the University must also be encrypted.

Examples of Breaches or Unauthorized Disclosures

Access to patient records when not involved in care of the patient	Stolen laptops containing unencrypted identifiable information
Paper records left in autos that are broken into	Flash drives left in computers with unencrypted data
Computers stolen from staff offices	Lost cameras or camera memory chips
Key stroke logger on email attachments	Email sent to wrong individuals
Faxes sent to the wrong fax number	

HIPAA Help

If you're confused about HIPAA, ask for help!

- UCR Health Compliance and Privacy Official or Campus General Counsel
- Your supervisor
- University's HIPAA website includes:
  - Notice of Privacy Practices
  - University's System-wide Standards and Implementation Policies
  - Authorization Form(s)
  - Business Associate Agreement
  - Other Education Modules

SCENARIOS

Scenario 1

The chief of cardiology reports to his assigned development officer that he has just treated the founder of a major Riverside company and asks the development officer to call the patient and discuss gift opportunities. *Is this a violation of HIPAA?*

Scenario 1 – Answer

The health care provider can provide information about the patient’s demographics and dates of service as well as academic department or service, treating physician, outcome information and health insurance status to the development officer, but cannot provide specific disease or treatment information. If the cardiologist would like the development officer to discuss specific treatment information with the patient, he should 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?*

Scenario 2 - Answer

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.

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 remittance envelope for gifts. *Is this a violation of HIPAA?*

Scenario 3 - Answer

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?*

Scenario 4 - Answer

The JDF is an outside entity. Providing a list of patients that is based on a disease and treatment protocol requires the patient’s Authorization.

Providing the list to JDF is an example of marketing and a violation of HIPAA, unless the patient has authorized the disclosure.

Scenario 5

The Cancer Center has built a new infusion center. It is working with its assigned development officer to invite the families of its chemotherapy 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?*

Scenario 5 - Answer

The answer used to be it was okay if you used the demographic information from all patients, but since we use a single registration system, you cannot select by where the patient had service or which physician the patient saw.

Scenario 6

The Development Office wishes to obtain lists of daily inpatient admissions and review them for prospective donors. *Is this a violation of HIPAA?*

Scenario 6 - Answer

As a part of healthcare operations, UA may use information that includes demographics and dates of admission as part of the development activities. It cannot identify location, treatment provider or any other information relating to treatment. Technically, you can review the lists, but how will you approach the patients? Will the patients think you are approaching them because you have knowledge about their disease? Will the public perception be that you have violated HIPAA?

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?*

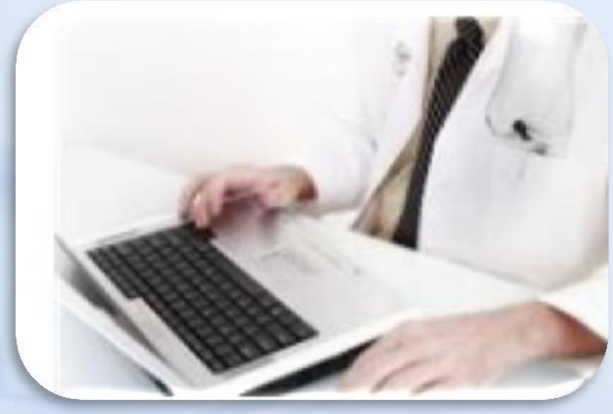
Scenario 7 - Answer

Technically, it may not be, but the public perception may be that UC is using disease-specific information to fundraise—a violation of HIPAA unless authorization has been provided. Volunteers are part of the UC workforce and should be trained that members of the workforce can only use a patient's demographics and dates of service—even when that patient is a friend—for fundraising. In some cases, the friend may have been a UC patient, and that could be a HIPAA violation. If a volunteer wants her friend to be contacted by the development officer, she should only provide the name, address and phone number AND advise the friend that she has done so.

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?



Scenario 8 - Answer

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.

Scenario 9

A Development Office staff member working on the Cancer Center campaign logs on to Advance because she wants to try to substantiate a tabloid story that a former UCI patient who is also a celebrity (and a major donor to the AIDS Research Institute) has AIDS. She finds PHI, along with a signed Authorization for fundraising, in advance and shares it with her family that evening. *Is this a violation of HIPAA?*

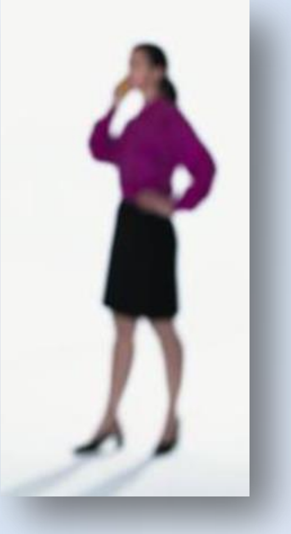
Scenario 9 - Answer

Yes, potentially 3 violations:

1) The medical center should have established a mechanism for preventing access to Advance 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 10

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?*



Scenario 10 - Answer

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 at this point.

Resources

Contact us at:

James Herron, Compliance & Privacy Officer
james.herron@ucr.edu
Phone: 951-827-4672

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!