

# Health Insurance Portability and Accountability Act (HIPAA)

*HIPAA Privacy Rule*

*Education Module for  
Institutional Review Boards*

HIPAA is federal law that applies to health care providers, health plans, and health care clearinghouses. These are covered entities (CEs).

The University of California is a hybrid Covered Entity with both covered and non-covered functions. All UC covered entities constitute a single health care component (SHCC).

The HIPAA Privacy Rule protects the privacy and security of an individual's health information held by a Covered Entity. 45 CFR sections 160, 164

The HIPAA Privacy Rule supplements the Common Rule and the FDA's protections for human subjects.

# Protected Health Information

## - PHI

### ◆ Health information

- Pertaining to an individual's past, present, or future:
  - ◆ Physical or mental health
  - ◆ Diagnosis and/or treatment
  - ◆ Payment for health care
- That includes **personal identifiers**, and
- That is created, used, or disclosed by a covered entity

# Personal identifiers under HIPAA are:

- ◆ Name
- ◆ Address including city and zip code
- ◆ Telephone number
- ◆ Fax number
- ◆ E-mail address
- ◆ Social security number
- ◆ Date of birth
- ◆ Medical record number
- ◆ Health plan ID number
- ◆ Dates of treatment
- ◆ Account number
- ◆ Certificate/license number
- ◆ Device identifiers and serial number
- ◆ Vehicle identifiers and serial number
- ◆ URL
- ◆ IP address
- ◆ Biometric identifiers including finger prints
- ◆ Full face photo and other comparable image

# Covered Entity's Responsibility

- ◆ The CE is responsible for protecting PHI
- ◆ The CE must ensure that PHI:
  - Is only used or released for treatment, payment or operations (TPO) and as permitted or required by law; or
  - If not used for TPO, is released only with the patient's authorization; or
  - If not used for TPO, is released only under an exception to the authorization requirement.

# HIPAA and Research

- ◆ Individually identifiable health information that is collected and used solely for research is NOT PHI.
- ◆ Researchers obtaining PHI from a CE must obtain the subject's authorization or must justify an exception to the authorization requirement:
  - Waiver of authorization
  - Limited Data Set
  - De-identified Data Set

# Conditions under which the CE may release PHI for research purposes

- Authorization by subject or subject's representative
- Waiver of authorization by IRB or Privacy Board
- Decedent research
- Limited data set
- De-identified data set
- Disclosures related to FDA-regulated product

Otherwise, you can't touch it!

# Impact of HIPAA on University Researchers

- ◆ To obtain PHI from a CE, a researcher must provide the CE with a Letter of Approval from an IRB or Privacy Board and one of the following:
  - Subject's Authorization to release PHI, or
  - Certification of Waiver of Authorization by IRB or Privacy Board, or
  - Request for Limited Data Set or De-identified Data Set
- ◆ The researcher may request from the CE only the minimum information necessary to conduct the research

# IRB's Responsibility

- ◆ Assure the CE that all research-related HIPAA requirements have been met:
  - Provide letter of approval to the researcher to conduct research with PHI
  - Certify and document that waiver of authorization criteria are met
  - Review and approve all authorizations and data use agreements
- ◆ Retain records documenting HIPAA actions for six years

# Subject's Authorization

- ◆ The authorization must include specific elements
- ◆ The authorization may be part of or attached to the research consent form
- ◆ An IRB or a Privacy Board must approve the language of the authorization
- ◆ The original signed authorization is retained by the CE; the subject gets a copy

# Authorization elements required by HIPAA

- ◆ Description of information to be used
- ◆ Name or class of persons authorized to disclose information
- ◆ Name or class of recipients of the information
- ◆ Description of research purpose
- ◆ Expiration date of authorization
- ◆ Right to revoke authorization
- ◆ That HIPAA protections may not apply to redisclosed information
- ◆ Consequences of a refusal to sign an authorization
- ◆ Signature and date

# Authorization expiration

- ◆ If the research has no expiration date, the authorization must state “no expiration date”
- ◆ Expiration may be a specific date or relate to the individual or to the purpose
  - “February 25, 2006”
  - “End of the research study”
  - “5 years after last patient is enrolled”
- ◆ After the stated date or event, researcher can no longer use the PHI

# Waiver of Authorization

- ◆ Investigator provides IRB approval of Waiver of Authorization to CE
- ◆ IRB approval provides:
  - IRB name, date of approval, brief description of PHI; and
  - Statement that IRB has approved Waiver of Authorization under normal or expedited review per Common Rule; and
  - Statement that IRB or Privacy Board has determined that research could not practicably be conducted without waiver and without PHI.

# Waiver of authorization (cont.)

- ◆ IRB approval also states that:
  - IRB or Privacy Board has determined that research poses no more than minimal risk to subject's privacy based on written assurance that the PHI will not be reused or disclosed, and
  - Researcher has provided adequate plan to:
    - ◆ Protect identifiers from improper use or disclosure; and
    - ◆ Destroy the identifiers unless retention is justified or required by law
- ◆ IRB or Privacy Board must retain documentation of waiver criteria for six years

**NOTE – the CE is responsible for providing an accounting to the subject of release of PHI under a research waiver**

# Limited Data Set (LDS)

## ◆ LDS may include:

- Zip code
- Full dates of birth or death
- Full date(s) of service
- Geographic subdivision (city)

## ◆ LDS may not include other personal identifiers of subject, relatives, employer, or household members

**NOTE – the CE does not have to account to the subject for disclosures using a limited data set**

# De-identification – Two Methods

- ◆ Remove all eighteen personal identifiers of subject, relatives, employer, or household members; or
- ◆ Biostatistician confirms that individual cannot be identified.

**NOTE –the CE does not have to account to the subject for disclosures using de-identified data**

# Use and Disclosure of PHI for Decedents Research

- ◆ Provide representation to the CE that the use or disclosure is solely for research on decedents' protected health information.
  - Similar to Waiver of Authorization
  - Requires approval by an IRB or a Privacy Board or a UC Privacy Officer

# Transition Rules for Research Protocols that Require the Subject's Consent and Authorization and that Use, Create or Disclose PHI

# Protocol approved before April 14, 2003

- If a study is active before April 14<sup>th</sup>, 2003, subjects enrolled before April 14<sup>th</sup> do not have to sign a HIPAA authorization or be re-consented
- If a study is active before April 14<sup>th</sup>, new subjects entered after April 14<sup>th</sup> must sign a HIPAA authorization addendum to the consent form
- UC authorization addendum language is provided by the IRB or Privacy Board
- The IRB or Privacy Board need not re-review the protocol so long as it is unchanged but for the authorization addendum

# Protocol modified or first approved after April 14, 2003

- ◆ If a study is modified or first approved after April 14<sup>th</sup>, 2003, subjects must sign a consent form containing HIPAA authorization language or a HIPAA authorization addendum to the consent form
- ◆ HIPAA authorization language that is embedded within a consent form must have a separate signature line from the informed consent signature line Cal.Civil Code 56.11

# Conclusion - HIPAA Privacy Rule

- ◆ Places responsibility on the Covered Entity to meet HIPAA requirements for disclosing PHI to a researcher
- ◆ Places responsibility on the IRB to assure the Covered Entity that health information will be protected under the research protocol.
- ◆ Does not replace Common Rule or FDA human subject protection regulations
- ◆ Does not override any California Law that provides greater protection for the privacy of health information.

If you have questions regarding the Privacy Rule, contact your campus' Privacy Officer or IRB Director