The Sixth National HIPAA Summit
Washington Hilton and Towers
March 28, 2003

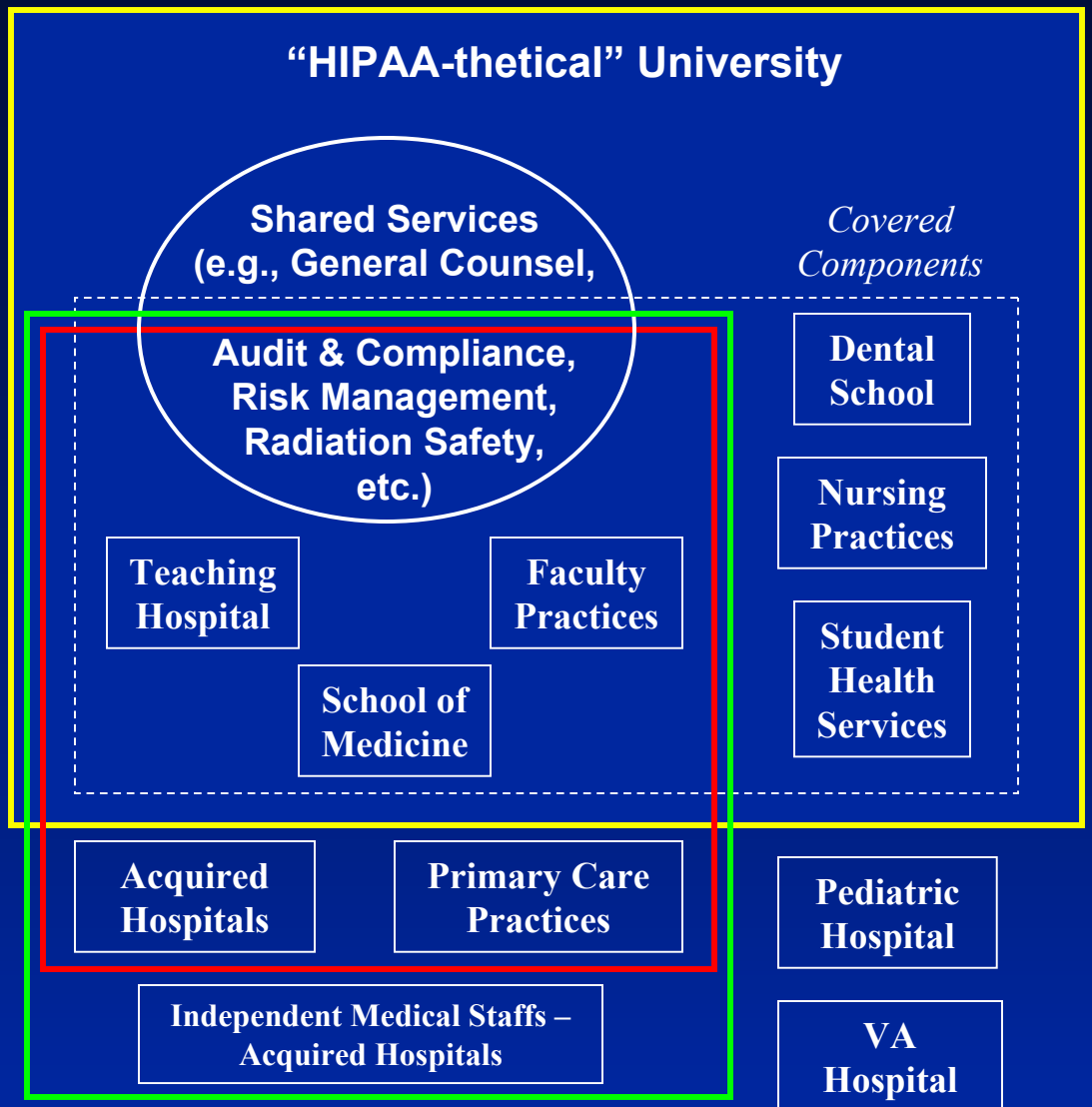
Session 3.02: Case Studies in Clinical Research Compliance

Russell M. Opland, M.P.H., EMT-P
Chief Privacy Officer and HIPAA Coordinator
University of Pennsylvania Health System
(215) 615-0643 oplandr@uphs.upenn.edu

What's a HIPAA?

What is our "Covered Entity" (CE)?

- Health plans
- Health care clearinghouses
- Health care providers who transmit any health information in electronic form in connection with covered transactions


"HIPAA-thetical" University
Shared Services (e.g., General Counsel, Audit & Compliance, Risk Management, Radiation Safety, etc.)
Covered Components
Dental School
Nursing Practices
Student Health Services
Teaching Hospital
Faculty Practices
School of Medicine
Acquired Hospitals
Primary Care Practices
Independent Medical Staffs – Acquired Hospitals
Pediatric Hospital
VA Hospital
__ - Hybrid
__ - ACE
__ - OHCA

Top 8 Reasons to Exclude Research

1. Privacy Rule is burdensome!
2. Reduced liability
3. Researchers not covered providers
4. Research not a covered function
5. No training required
6. Exclusion from Designated Record Set
7. No electronic transactions
8. Already covered by Common Rule

Top 8 Reasons to Include Research

1. No Accounting requirement for Uses
2. Uses preparatory …
3. Clinicians are researchers
4. Include co-investigators
5. If excluded, firewalls required
6. Clinical databases often used for research
7. Privacy Rule represents “Best Practice”
8. Electronic billing is conducted

Implementing firewalls

- Organizational Unit method
  - Schools, departments
- Clinical vs. basic sciences
- Project method

Use and Disclosure of PHI

- Authorizations
- Waivers of Authorization
- Limited Data Sets
- De-Identified Data

- Uses preparatory …
- Decedents

Common Rule vs. Privacy Rule

Applies to *federally supported* or *FDA regulated* research	Applies to *all* research
Protects *rights* and welfare	Protects *privacy* rights and welfare
Human subject: A living individual about whom an investigator obtains (i) data through intervention/interaction or (ii) identifiable private information; or An individual who participates in research involving a test article	*Individual*: subject of information; a living or deceased person
Uses Institutional Review Boards (IRBs)	Uses IRBs or Privacy Boards
Board reviews all non-exempt human subject research	Board reviews only authorization waivers or alterations
Continuing review at least annually	*No requirement for continuing review*
Informed Consent	Authorization and Consent

Authorizations

- Authorization must include the following Required Statements:
  - The individual's right to revoke the authorization, including exceptions, and reference to Notice of Privacy Practices
  - Covered entity (CE) may continue to use PHI pursuant to authorization if the CE has already acted in reliance upon the authorization
  - For research, CE may continue to use to protect the integrity of the research, e.g., to conduct a scientific misconduct investigation

Authorizations

- Individual Authorization is a one-time individual permission to use or disclose PHI for non-TPO activities
- Authorization must include the following Core elements:
  - Description of the PHI in a specific and meaningful manner
  - Name, identification, or class of individual(s) authorized to use or disclose PHI
  - Name, identification or class of person(s) to whom PHI may be disclosed
  - Description of each purpose of the use or disclosure
  - An expiration date or event (may be “none” or “end of research project”)
  - Individual Signature

Authorizations

- Covered entity's ability or inability to condition TPO on authorization:
  - General prohibition from conditioning treatment, payment, enrollment or eligibility of benefits on provision of authorization (except under certain clinical research requirements)
  - CE may condition research-related treatment upon the individual's authorization
- Statement of the potential that information disclosed pursuant to the authorization may be re-disclosed by the recipient and the information is no longer protected by HIPAA

Transition Issues

- New studies: probably use combined Authorization
- Existing studies still recruiting: probably use new, separate Authorization
- Existing studies not recruiting: generally grandfathered

Authorization/Consent Issues

- IRB not required to review if separate
- If separate, IRB should ensure consistency with Informed Consent
- FDA-regulated sponsors may prefer separate to avoid liability
- Allows continued use of info and follow-up if patient withdraws and doesn't revoke

Waiver Criteria

1. Use or disclosure involves no more than minimal risk to the individuals:
    a. There is an adequate plan to protect the identifiers from improper use and disclosure;
    b. There is an adequate plan to destroy the identifiers at the earliest opportunity, unless there is a health or research justification for retaining the identifiers or if otherwise required by law; and
    c. There are adequate written assurances that the PHI will not be reused or disclosed, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by the rules.

Waiver Criteria

2. The research could not be practicably conducted without the waiver; and

3. The research could not be practicably conducted without access to the PHI.

IRB Waivers

- IRB Waivers may be accepted by another CE
- Waivers may be used to obtain verbal authorization (e.g., at-risk youth, domestic violence studies, phone surveys)
- IRB or Privacy Board documentation requires:
  - Signature of chair of IRB or PB, or designated member;
  - Identification of IRB or PB;
  - Identification of the PHI approved for use or disclosure; and
  - Specify the review procedures.

Limited Data Sets

- The limited data set is PHI without facial or direct identifiers
- Facial identifiers include: (1) name; (2) street address (renamed postal address information, other than city, State and zip code); (3) telephone and fax numbers; (4) e-mail address; (5) social security number; (6) certificate/license numbers; (7) vehicle identifiers and serial numbers; (8) URLs and IP addresses; and (9) full face photos and any other comparable images
- Other facial identifiers that must be removed to form the LDS include: (1) medical record numbers (prescription numbers), health plan beneficiary numbers, and other account numbers; (2) device identifiers and serial numbers; and (3) biometric identifiers, including finger and voice prints

Limited Data Sets

- Identifiers that may be used in the LDS include:
  1. Information related to dates, including dates of admission, discharge, birth, death;
  2. Geographical information such as city, state, five-digit zip code; street address is not permitted in the limited data set;
  3. "Any other unique identifying number, characteristic or code"
- The Limited Data Set may only be used for research, public health, or health care operations

Data Use Agreements

- Before disclosure of the Limited Data Set, the covered entity must obtain from the recipient a Data Use Agreement which specifies:
  - Permitted uses and disclosures of the information in the LDS
  - Uses must be consistent with research, public health or health care operations
  - Limits who can use the data
  - Requires the recipient not to re-identify the information or contact the individuals, and
  - Contains adequate assurances that the recipient use appropriate safeguards to prevent use or disclosure of the limited data set other than as permitted by the Rule and the data use agreement, or as required by law.

De-Identified Data

- Individually identifiable health information from which identifiers are removed for the individual, *and their relatives, household members, or employers*

De-Identification Requirements

(A) Names;
(B) Street address, *city, county, precinct, zip code, and equivalent geocodes*;
(C) *All elements of dates (except year) for dates directly related to an individual and all ages over 89*;
(D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses;
(G) Social security numbers; (H) Medical record numbers;
(I) Health plan ID numbers; (J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers/serial numbers; (N) Web addresses (URLs);
(O) Internet IP addresses; (P) Biometric identifiers, incl. finger and voice prints;
(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying number, characteristic, or code.

- **Note: additional detailed exceptions and restrictions apply**

De-Identification

- May use link field, but may not be derived from PHI (e.g., DOB, SSN)
  - CE may retain index
- Age ≥ 90 becomes one category
- Freed from Privacy Rule

Accounting for Disclosures

- Not required for Uses, Authorizations
- Three options:

1. Each individual disclosure; or
2. Range of disclosures to same person or entity for a single purpose; or

Accounting for Disclosures

3. For research disclosures involving 50 or more individuals:
   - Name of protocol
   - Description of protocol, *including purpose and selection criteria*
   - Type of PHI disclosed
   - Date or period of disclosures
   - *Name, address, phone number of researcher and sponsor*
   - "PHI may or may not have been disclosed"

CE shall assist in contacting researcher and sponsor

Sponsor Issues

- Sponsors generally not
  - Business Associates
  - Covered entities
- Concerns re: sponsor protection of PHI
- Sponsors generally opposed to BA Agreements or Data Use Agreements
- Suggest including language in contract
  - e.g., bind sponsor to terms of Authorization

Research Databases

- Who “owns”?
  - Covered Entity?
  - Provider?
  - Researcher?
  - Patient?
- How to locate, track, and control?

Research Databases

- Case logs held by clinicians
  - Usually residents in surgery or highly technical sub-specialties for board certification (may be health care operations, but concerned re: disclosure)
  - Cases sometimes submitted to registries (will likely require Authorization)

Research Databases

- Databases collected for future, unspecified use
  - Can create databases with Waiver or Authorization
  - Comply with requirements to Use
  - Control of databases when faculty leave
  - Cultural challenge
  - Tissue or blood samples

Recruitment

- Covered under activities preparatory …
- Some still prefer waiver
- Theoretically anyone within Covered Entity may contact
- Recommended method:
  1. Direct contact by treatment provider
  2. IRB-approved letter from treatment provider
  3. Direct contact from researcher
- Verbal consents under waiver

Business Associates

- Permitted for research activities
- May be used to de-identify data
- May be used for data aggregation for health care operations
- Commercial IRBs or Privacy Boards
- Accounting requirement for non-TPO disclosures

Activities Preparatory / Decedents

- In preparation for research (e.g., protocol preparation) or reviews of decedent information, the covered entity must obtain from the researcher:
  - Representations that the use or disclosure is sought solely to prepare a research protocol or for similar purposes preparatory to research, or for research of PHI of the decedent;
  - Documentation of the death of the individual;
  - Representations that *the PHI will not be removed from the covered entity*;
  - Representation that the PHI used or accessed is necessary for the research purpose.

Questions / Discussion?