HIPAA and PHI: Approvals, Waivers, Transferring Data, and the Medical Record

Lawrence H. Muhlbaijer, PhD
Duke Clinical Research Institute
Biostatistics & Bioinformatics

27 Mar 2013
DOCR "Research Wednesday"

Structure of Session

- What's New
- Case Studies
- Some HIPAA Basics
- Transferring Data
- References
- Additional Topics (only if questions)

New Stuff – 1

- "Omnibus" HIPAA Regulation Update came out in January
- Fortunately, few changes for Research
- Changes must be in place by September 20, 2013
New Stuff – 2

- Allows "opt in" check-boxes to be used in any Consent/Authorization.
  - IRB Policy still requires separate consent/authorization for "banks."
  - No changes to other consent language.
- Individuals dead > 50 years are no longer covered.

New Stuff – 3

- Updated Notice of Privacy Practices will need to be provided
- New breach reporting requirements
  - may require reports to research participants
- New Business Associate Agreements
  - Few used in research

Case Study 1

- A Duke investigator is studying the occurrence of arrhythmias after discharge from an AFib Ablation procedure.
Case Study 1

iRhythm makes a device that can be worn for 2 weeks and records heart rhythm events (like a mini-Holter). It's small (the size of a bandaid) and doesn't have any external wires, etc.

Case Study 1

- The PI puts the device on the subject and activates it.
- The data on the device are PHI.
- After 2 weeks, the subject peels it off and sends it to iRhythm for reading.
- iRhythm posts the results on the web for the PI to read.

Case Study 1

- How do we (Duke and the PI) handle this so the regulations are followed, and the subject’s rights are respected?
Case Study 2

- A fellow is working on a research project with the PI and copies the data to a flash drive so she can work on it at home over the weekend. The data include MRN, name, and DoB.
- Her car is broken into and the backpack with the flash drive, her computer, and more are taken.

Case Study 2

- What should she do?
- What are the side effects?
- What could she have done differently?

Case Study 3

- A PI used the "standard language" and said that only coded identifiers would go to the sponsor.
Case Study 3

CONFIDENTIALITY
Study records that identify you will be kept confidential as required by law. Federal Privacy Regulations provide safeguards for privacy, security, and authorized access. Except when required by law, you will not be identified by name, social security number, address, telephone number, or any other direct personal identifier in study records disclosed outside of Duke University Health System (DUHS). For records disclosed outside of DUHS, you will be assigned a unique code number. The key to the code will be kept in a locked file in Dr. [PI]'s office.

However, he sends SSNs so they can do National Death Index searches.
This is discovered in an audit.

How is this different from CS 2?
What happens to the PI and the study?
What should have been done?

Some HIPAA Basics
What is HIPAA?
- Health Insurance Portability and Accountability Act (1996)
- Last vestige of Bill Clinton's Universal Health Care
- Portability: Take insurance to next job
- Accountability: Fraud prevention
- NO mention of Privacy!!!

What was the law trying to solve?
- Portability
  - Prior to HIPAA, a new employee could be denied (group) health insurance for pre-existing conditions.
  - Locked people with chronic diseases into one company
  - Stifled job changes and productivity

What was the law trying to solve? -- 2
- Accountability
  - CMS felt they needed more tools to address false billing practices.
  - Included good-faith overcharges as well as outright fraud.
What was the law trying to solve? -- 3

- Privacy
  - Uniform electronic billing
  - Prior to HIPAA, Duke paid electronic bills in >200 different formats
  - Hospital requested the uniform billing
  - With mandated format came responsibility to protect information

What was the law trying to solve? -- 4

- Privacy (continued)
  - Under "administrative simplification"
  - Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit ... detailed recommendations on standards with respect to the privacy of individually identifiable health information.

What was the law trying to solve? -- 5

- Privacy (Continued)
  - 12 Months became 7 years: Why?
  - Congress couldn't do it. (privacy for minors and abortion too "hot" for them)
  - HHS had 3 more years
  - First proposal drew 52,000 comments
    - too strict
    - too lenient
What was the law trying to solve? -- 6

- Privacy (continued)
  - HHS wrote regs as broadly as possible under the law.
  - Applies to individuals, not just patients

What was the law trying to solve? -- 7

- Privacy (Continued)
  - Remember the 200 formats?
  - Changing to one format saved Duke much, much more than the cost of implementing privacy and security to meet HIPAA
  - (of course it's different 'pockets')

What was the law trying to solve? -- 8

- Security
  - A tool (one of many) to enable privacy controls
  - Security Reg a bit better structured than Privacy Reg
    - Requires a risk analysis and development of policies to mitigate the risks.
Other federal Privacy & Security Regulation

- Privacy and Security regulations are already in place for
  - Banking
  - Interstate commerce activities
  - Federal Gov (Privacy Act of 1974)
  - EU "Safe Harbor" for commerce

Note on nomenclature

- Privacy
  - control of information
- Confidentiality
  - protection of entrusted information
- HIPAA is really about confidentiality, but many federal regulations use "privacy" and "confidentiality" interchangeably

Ethical Concerns

- Privacy (Confidentiality)
- Automation ↑↑ Volume of Violations
Examples of Lapses
- Carolina Mammography Registry (UNC)
- Stolen laptop. Stanford. 57,000 patients being notified. 1/9/2013.
- Back-up Tapes stolen from courier
- Student records left open on web site
  - Many universities
  - Duke Law
- http://www.privacyrights.org/

Privacy, as Embodied in HIPAA
The right to control personal information even after disclosing it.
Balanced with the public good.

Individual Rights under HIPAA
- Request restrictions on disclosures
- Confidential communications
- Access to Protected Health Information (PHI)
- Amendment of PHI
- Accounting of disclosures
How do these rights fit in?

- Request restrictions on disclosures
- Confidential communications
- Access to Protected Health Information (PHI)
- Amendment of PHI
- Accounting of disclosures

HITECH Act Enhances Rights

- Restrictions – Individual can block Insurers from seeing certain sections of records
- Disclosure Accounting – shortened time, broadened scope
- (New) Access Accounting
- Breach Notification – for any use of disclosure outside the scope of the rule

What is PHI?

- PHI = Protected Health Information
- Relates to past, present, or future health, health care, or payment for health care
- Identifies the individual, directly or indirectly
- Held by a CE
- (Not necessarily part of clinical process)
Covered Entity Activities that Affect Research

- Privacy Notice -- use/disclosure for research
- Include Research Disclosures in disclosure accounting system
- Security provisions apply to research data as well as care data.

Research Authorizations

- "Contract" with individual
- Allows uses and disclosures that could not otherwise be done under HIPAA

Elements of an Authorization to Use or Disclose PHI

Core Elements:
- Description of PHI to be used or disclosed
- Person(s) authorized to make the requested use or disclosure.
- Person(s) to whom the covered entity may disclose PHI
- Each purpose for the use or disclosure.
- Expiration date or event (e.g., "end of the research study" or "none").
- Signed copy to individuals

Statements:
- Right to revoke Authorization plus exceptions and process.
- Ability/Inability to condition treatment, payment, or eligibility for benefits on Authorization.
- PHI may no longer be protected by Privacy Rule once it is disclosed by the covered entity.
- If data to be withheld for study, tell them and when it will be available (e.g., Randomized Tx)

Participant Signature

Date
Other ways to use data for research under HIPAA

- Waiver or alteration of authorization
- Notice of Review Preparatory to Research
- Notice of Decedent Research
- Limited Data Set/Data Use Agreement
- De-Identification

Research Challenges from HIPAA

- If also covered by Common Rule (much of what we do is), the regs overlap but are enough different that it is sometimes hard to mesh them together.
- Relatively new regulation – interpretations still vary (headache for multisite research)

Research Challenges from HIPAA – 2

- More paper (research authorization language).
- More complex consent/authorization forms.
- More institutional bureaucracy.
Transferring Data

- Gil Smith covered this on March 13

The Medical Record

- Is PHI, as are study CRFs.
- Release can be included in the ICF
- Can be used for pre-screening, under a Waiver
- Can be used for other research (chart "review", DEDUCE)

Resources on the WEB

- Duke IRB
  - [http://irb.mc.duke.edu](http://irb.mc.duke.edu)
  - [http://eIRB.mc.duke.edu](http://eIRB.mc.duke.edu)
  - Download eIRB Forms → HIPAA Forms
- Duke General HIPAA Info
  - [http://hipaa.duke.edu/](http://hipaa.duke.edu/)
  - Duke Health Notice of Privacy Practices
    - [http://www.dukehealth.org/Privacy/privacy](http://www.dukehealth.org/Privacy/privacy)
- NC Healthcare Information & Communications Alliance
  - [http://www.nchica.org](http://www.nchica.org)
Resources on the WEB

- NIH Fact Sheets
  - http://privacyruleandresearch.nih.gov/
- Federal Gov’t Site
  - http://www.hhs.gov/ocr/hipaa/

People Resources at Duke

- Security:
  - Each workgroup has a designated Security Manager
  - Usually called via computer support people
- Privacy:
  - Workgroup Privacy Manager
  - Business Managers should know who that is
- SoM Compliance Office

Contact Information

Doc Muhlbaier
919-668-8774
lawrence.muhlbaier@duke.edu
Additional materials follow

- These will not be covered unless questions.

Database Research Considerations

- Waiver of Authorization/Consent
- Use vs Disclosure
- Minimum Necessary
- De-identification vs Anonymization
- Disclosure Accounting

Use vs Disclosure

- Use
  - Within the CE
  - Soon to be tracked for accounting to individual
- Disclosure
  - Outside the CE
  - Includes sponsors, outside contractors
  - If not TPO or with Authorization, tracked for accounting to individual
Preparing for Research

- Study Sizing
- Qualifying for procedures
- Grant preparation
- Pre-Screening
  - (if NOT under “Common Rule”)

Reviews Preparatory to Research

- Requires notification of ‘covered entity’
- No PHI may be removed from CE
- PHI required for the review
- PHI can only be used for the review
- (May still be a disclosure)

Identifying Patients for Study:
"Case Finding" or "Pre-Screening"
Four Methods

1. Operations
2. Reviews Preparatory to Research
3. Waiver of Authorization
4. Direct contact (ads, web)
Operations or Reviews Preparatory to Research

- Limited value if research also subject to Common Rule
  - HHS has stated that such case identification is part of research and requires a waiver or consent
- Waiver more robust and flexible, but harder to make changes.

Pre-Screening – Waiver Implications

- IRB needs to know if sponsor gets or sees PHI from Pre-Screening
- ID removal requirement implies contract modifications with sponsor
- Disclosures require tracking

Recruiting with Ads (print, web, ...)

- For Pre-Screening:
  - No Notice of Review Preparatory to Research
  - No Waiver of Authorization
- Enrollment:
  - Waiver (Alteration) of Authorization (HIPAA)
  - Waiver of Doc. of Consent (Common Rule)
  - Provide Notice of Privacy Practices (Maybe)
Research Without Authorization

- Pilot Studies
- Medical Records Studies
- Health Services Research
- Other areas "impracticable" to obtain authorization
  - Includes telephone surveys

Research Without Authorization (e.g. Medical Records Study, Registry, Health Services Research)

- May use/disclose as described in IRB protocol
- Minimum Necessary applies
- Other use requires new review
- Disclosure accounting necessary

Anonymization vs De-Identification

- IRB vs HIPAA
  - Both require deletion of direct identifiers.
  - Anonymization cannot have a link field, De-ID can.
  - Anon can have full dates, De-ID can only have true year.
  - Anonymization makes protocol eligible for exemption from IRB review.
  - De-ID makes data exempt from HIPAA regulations.
De-Identification (Safe Harbor)

- Delete or modify 18 specific items
- Limited Geocoding (State, part ZIP)
- Dates are Year only
- Age > 89 → Age = 90
- If link-field included, still requires IRB review ("coded" or "linked", not anonymized)*

Limited Data Set (with Data Use Agreement)

- Remove direct identifiers
- Can have dates, more geocodes (ZIP, ZIP+4, census tract, city)
- Requires "contract" with recipient
- If link-field included, still requires IRB review*

* Research on Coded Data


Allows Coded data to be declared “not Human Subjects,” under certain circumstances.
Research on Decedent PHI

- Now covered as any other PHI
  - Individuals dead > 50 years excluded
- Requires ‘notification’ of CE (IRB)
  - Implementation requires response
  - May need evidence of death
- Tracking needed for accounting of disclosures

Disclosure Tracking (For accounting to individual)

- Requires
  - Who (PI)
  - Why (Title)
  - to Whom (Sponsor)
  - When
  - What
- At Duke:
  - https://clinapp1.duhs.duke.edu:8081/phidisclosuretracking/Authenticate.asp

What Disclosures to Track?

- Monitor reviews (even if nothing removed)
- Pre-screening logs submitted to sponsor (limited data set easier)
- Outside Audits (e.g. FDA)
- PHI from Waiver sent outside CE
When A Laptop Goes Missing.....

Compliance Investigation

- Notification Compromise Scoring (to determine need to notify individuals and HHS/Media)
  - Breach Review
    - Interviews with those involved
    - Describe events
      - Summary
        - Document notification to individual
          - Document notification to HHS
          - Document notification to media

- Disclosure accounting documented for each individual whose data were disclosed
  - https://clinapp1.duhs.duke.edu:8081/phidisclosuretracking/Authenticate.asp
  - Discipline ("Written Counseling" is minimum)
  - http://www.hr.duke.edu/policies/expectations/phi.php
Contact Information

Doc Muhlbaier
919-668-8774
lawrence.muhlbaier@duke.edu