New HIPAA Privacy Regulations Governing Research

Karen Blackwell, MS
Director, HIPAA Compliance
kblackwe@kumc.edu
913-588-0942
HIPAA

- Health
- Insurance
- Portability and
- Accountability
- Act
“In a Nutshell”

The Privacy Regulations govern a provider’s use and disclosure of health information and grant individuals new rights of access and control. The regulations also establish civil and criminal penalties for violations of patient privacy.
The History of the Privacy Rule

- Proposed - November 1999
- Finalized - December 2000
- On Hold – February 2001
- “Effective” – April 2001
- Guidance – July 2001
- Proposed changes – March 2002
- Modified Final Rule – August 2002
- More Guidance – October 2002
- Much More Guidance – December 2002
HIPAA: The Terminology

- Covered entity
- Protected Health Information (PHI)
- Use and disclosure
- Role-based access
- Minimum necessary
Covered Entities

- Health plans
- Health care clearinghouses
- Health care providers who conduct electronic transactions related to third-party billing
Protected Health Information (PHI)

- Relates to past, present, or future health, or health care, or payment for health care
- Identifies the individual, directly or indirectly

*PHI can be paper, electronic, or oral. Examples include clinic charts, billing records, rounding lists, medical media, clinic or research databases, and hallway conversations.*
Use and Disclosure

“Uses” occur within the covered entity

“Disclosures” are releases outside the entity that is responsible for holding the information
Role-based Access

- Identify the persons or classes of persons who need access to PHI, and the categories of PHI that they need access to, in order to carry out their duties.

- Covered entities must limit the PHI used or disclosed to the minimum necessary to achieve the purpose of the use or disclosure.
  - Doesn’t apply to disclosures made for treatment or to the individual
Minimum Necessary

- Make reasonable efforts not to use, disclose, or request more than the minimum amount of information necessary to achieve the purpose.
- In the research context, this applies to studies that do not obtain written authorization from the subject.

Examples: recent visits instead of the entire Medical Record; age instead of DOB.
Basic Requirements:
Research Issues

- New review process for privacy issues
- HIPAA requirements are in addition to Common Rule regulations
- HIPAA governs how PHI is used for research and the conditions that must be met in order for covered entities to release PHI for research purposes
Underlying Principles for Privacy

- Health information belongs to the patient
- Patients have a right to know how their information is being used.
When does HIPAA apply to research?

The rules apply if we access PHI to initiate the study or if we create PHI during the course of the study.
What makes it PHI?

Health Info + Identifying Elements

- Names
- Street address, city, county, precinct, zip code
- Dates (e.g. DOB, DOD, admission, discharge, procedure dates)
- Ages over 89
- Phone and numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record number
- Health Plan Numbers
- Account numbers
- Certificate/license numbers;
- VIN/License plate number
- Device identifiers and serial numbers
- URLs
- Internet Protocol (IP) address
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images;
- Any other unique identifying number, characteristic, or code
Allowable Conditions for Use of PHI in Research

- Obtain written authorization from the patient

OR

- Meet one of the following criteria:
  - De-identified data
  - IRB waiver of individual authorization
  - Limited data set + data use agreement
  - Activities that are “preparatory to research”
  - Research on decedents
Required Elements for Authorizations

- A specific description of the purpose of the authorization and the information to be used or disclosed
- The names or classes of individuals authorized to make the use or disclosure
- The names or classes of individuals authorized to receive the use or disclosure
- An expiration date for the authorization
- A statement that the individual has a right to revoke the authorization
- The consequences of refusal to sign
- A statement that the information used or disclosed pursuant to the authorization may be subject to re-disclosure and no longer protected by the Privacy Rule.
Conditions Not Requiring Authorization

- De-identified data
- Waiver of authorization by an IRB or Privacy Board
- Limited data sets
- Activities that are “preparatory to research”
- Research on decedents
De-identified data

- All eighteen identifiers must be removed
- Not necessarily designed for research purposes
- If you are accessing or receiving only de-identified data for your project, HIPAA rules do not apply.
Waiver of the Authorization Requirement*

**Examples:** retrospective chart review; accessing medical records to screen subjects for a clinical trial

Application for waiver must be approved by an IRB or Privacy Board

Use and disclosure poses no more than minimal risk to privacy
- Adequate data protection plan
- Adequate plan to destroy identifiers
- Adequate assurances against re-use or disclosure

Research is not practicable w/o waiver

Research is not practicable w/o PHI

*DHHS has promised more guidance on implementation of the waiver criteria.*
Limited data set

Example: receiving tissue samples w/ partial identifiers

Remove certain “direct identifiers”
- Name, street address, phone, fax, email, IP, SSN, MR#, insurance and billing #, device serial numbers, full-face photos, biometrics

(DOB, service dates are OK; City, zip code, precinct are OK)

Provide a Data Use Agreement
- Specific uses and planned disclosures
- No further disclosures allowed
- Agreement not to identify or contact individuals
Preparatory to Research

**Example:** reviewing medical records to determine adequacy of patient base

- PHI may be viewed, but only de-identified data can be **recorded**.
- Covered entity must obtain an attestation from the researcher:
  - Review of PHI is solely to prepare a protocol or formulate hypotheses
  - PHI will not be removed from the covered entity
  - PHI being reviewed is necessary for research purposes

- This activity generally precedes HSC application, if there is no formal protocol developed.
Research on Decedents

Covered entity must obtain an attestation from the researcher:
- Research is solely on decedents
- PHI is necessary for research purposes

Covered entity may stipulate that documentation of death be provided
GRANDFATHERING
- If the consent is already signed, study visits and data collection may continue.
- Existing databases may continue to be accessed, if the data was collected under a consent or waiver of consent.

HIPAA review will happen during HSC review.
Starting 4/14, anyone who is consented or re-consented on a study MUST sign a privacy authorization
Exempt studies that collect data after 4/14 need a privacy review.
New recruitment practices
Appropriate documentation must be presented to the holder of the medical record in order to access PHI for research
Some implementation procedures are institution-specific.
Recruitment Questions

- Are you using PHI to identify subjects?
- If so, what permissions do you need to gain access to the PHI?
- Do you have a treatment relationship with the prospective subject?
Allowable Recruitment Practices

- Providers can always talk to their own patients about studies they are conducting.
- Providers can notify the patient that they might qualify for a particular study, and the patient can initiate the contact with the researcher.
- Provider or Medical Records Dept. can release information to researchers if:
  - The patient signs a pre-approved authorization so that the provider can give PHI to researcher, or
  - The IRB approves a partial waiver of authorization for recruitment purposes. (The HIPAA waiver criteria must be met.) Researcher identifies subjects, and member of treatment team makes initial contact.
- Patients can self-refer from ads, flyers, etc.
Other Issues

- Pre-screening logs
- “Future unspecified research”
- Research repositories
- Accounting of disclosures
- Subjects’ access to the research record
- Computer security for research records
Pre-screening Logs

- PHI in logs cannot be disclosed because consent has not been obtained.
- Options include de-identification or negotiation of a Data Use Agreement.
Future Unspecified Research

“Future unspecified research” will no longer be allowed

Consents for tissue, blood banking, etc. need to be specific

Contacting subjects for future studies must follow new recruitment guidelines
Research Repositories

Creation of a research repository requires HSC approval: allowed with written authorization, waiver, or a limited data set.

Subsequent studies using the repository must go through HSC.
Accounting Requirement

- Covered entities must track disclosures made under a waiver of authorization, a review preparatory to research, or research on decedents.
- Patients may request the name of the study, the purpose of the study, type of PHI disclosed, timeframe of disclosure.
- HIPAA Compliance Office will assign a tracking number.
Patients have the right to access their “designated record set” – the set of medical and billing records that are used to make decisions about them.

Any temporary denial of access must be accepted by the patient.

Research records generally are not part of the designated record set.

Be sure to put any clinically-relevant information into the medical record.
Computer Security for Research Records

- Practice role-based access
- Password-protect files
- Store records on secured networks or servers
- Obtain certification for hard drives that contain PHI
Planning Your Study

- What type of data do you need?
- What’s the minimum necessary?
- Who holds the data you need to access?
- How will you identify subjects?
- What data protections will you put into place?
Stay Tuned!

We’re just beginning, and the government is planning changes.
April 14, 2003

Office of HIPAA Compliance
Karen Blackwell, MS
Tom Field, MSEd, MHSA
913.588.0942

www.kumc.edu/hipaa/research