HIPAA Privacy & Security: Medical Research Context

Medical Research Summit
Washington, DC

March 25, 2002

Bill Braithwaite, MD, PhD
Director

The Privacy Rule: Research Provisions

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

(Definition from the 'Common Rule')

Debate about effect of new federal medical privacy rule on research:

- 2 articles in January 17, 2002 issue of NEJM
- Opposing viewpoints well expressed.

Debate over privacy rule -

CON:

- Complex, burdensome, and costly
- Ambiguous
- Too specific (de-identification, notices, and authorizations)
- Fear of liability – enforcement
  - (potential suspension of research programs)
- Unnecessary (no research breaches)
- Need new comprehensive health information privacy law.

PRO:

- Inform patients, give them control, restore trust
- High level of public concern about research and medical records.
- More people will be willing to participate in confident
- No HIPAA provisions impede research - reasonable
- Clarifications may be needed

Types of Research

Two forms of research are affected:

1. Research that only uses protected health information (PHI)
   - either with or without individual authorization.
2. Research that includes treatment of research participants.

“Covered Entities”

1. Health care **providers**
   - who transmit health information in electronic form in connection with a HIPAA transaction,
   - Including providers who disclose information to researchers.
   - Including researchers who provide treatment to research participants.
2. Health **plans**
3. Health care **clearinghouses**

Covered Information

Individually identifiable health information, in any form or medium, that is created or received by a health care provider, health plan, employer or health care clearinghouse.

- Becomes PHI in hands of ‘covered entity’

De-identified health information is NOT covered.

Using PHI for Research Purposes

5 ways PHI can be used for research:

1. De-identified PHI
2. PHI with IRB/Privacy Board waiver
3. PHI for research protocol preparation
4. PHI of deceased
5. PHI with authorization of subject

plus, Healthcare Operations, Public Health, and as otherwise required by law (registry, reportable).

De-identified Information

A covered entity may determine health information is not individually identifiable under two circumstances…

1. The ‘statistical’ method
2. The ‘safe harbor’ method

‘Statistical’ De-identification

A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that :

- **the risk is very small** that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual;
- OR…

‘Safe Harbor’ De-identification

Identifiers are removed:

- Names
- Geographic subdivisions smaller than a State (except 3 digit zips)
- All elements of date (except year) for dates directly related to the individual
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- SSNs
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- VIN and serial numbers, license plate number
- Device identifiers and serial numbers
- URLs
- Internet Protocol address numbers
- Biometric identifiers
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code

PLUS…

The covered entity must not have **actual knowledge** that the information can be used alone or in combination with other information to identify the individual.

De-identified information may include:

- re-identification codes
- ages (<90)
- date differences (e.g. LOS, time since diagnosis)

Research Use and Disclosure of PHI **WITHOUT** Individual Authorization

Permissible under three circumstances:

1. obtain documentation that an IRB or privacy board has determined specified criteria for a **waiver** were satisfied;
2. obtain representation that the use or disclosure is necessary to prepare a research protocol or for similar purposes **preparatory to research**;
3. obtain representation that the use or disclosure is solely for **research on decedents'** PHI.

8 Waiver Criteria
(1st 3 same as Common Rule)

1. Use or disclosure involves no more than minimal risk to the individuals;
2. Waiver will not adversely affect the privacy rights and the welfare of the individuals;
3. Research could not practicably be conducted without the waiver;
4. Research could not practicably be conducted without access to and use of the PHI;
5. Privacy risks are reasonable in relation to

- the anticipated benefits, if any, to individuals, and
- the importance of the knowledge that may result;

8 Waiver Criteria (continued)

6. There is an adequate plan to protect the identifiers from improper use and disclosure;
7. 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

8. 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.

Research Use and Disclosure of PHI **WITH** Individual Authorization

The Privacy Rule **does not** override the Common Rule or FDA's human subjects regulations.

For research that is subject to the Privacy Rule and above, both individual authorization AND informed consent are required.

- May be in same document.

Requirements for Individual Authorization

If initiated by the prospective research subject, must contain 8 core elements.

If initiated by the covered entity for its own uses and disclosures (e.g., for research), must contain the 8 core elements plus 4 additional elements.

8 Core Elements of Authorization

1. A specific and meaningful description of the information to be used or disclosed;
2. The name or other specific identification of those authorized to make the requested use or disclosure;
3. The name or other specific identification of those to whom the covered entity may make the requested use or disclosure;
4. An expiration date or an expiration event;
   - Event may be the termination of the research study

8 Core Elements of Authorization

5. A statement of the individual's right to revoke the authorization;
6. A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure and no longer protected by [HIPAA];
7. Signature of the individual and date; and
8. If the authorization is signed by a personal representative, a description of the authority to act for the individual.

4 Additional Elements (when entity asks for authorization)

1. a statement that the covered entity will not condition treatment on the individual's providing authorization for the requested use or disclosure;
   - Unless treatment is research related
2. a description of each purpose of the requested use or disclosure;
3. a statement that the individual may:
   - Inspect or copy the PHI to be used or disclosed, and
   - Refuse to sign the authorization; and
4. if use or disclosure of the requested information will result in direct or indirect remuneration to the covered entity from a third party, a statement that such remuneration will result.

Research Use and Disclosure of PHI for Research that **Involves Treatment**

Researcher must obtain research subjects' authorization for any uses or disclosures of "research PHI" not permitted by the Rule without authorization.

Authorization for research that involves treatment must include three elements:

Three authorization elements for Research involving Treatment

1. A description of the extent to which such PHI will be used or disclosed to carry out treatment, payment or health care operations;

2. A description of any PHI that will not be used or disclosed for purposes permitted by the privacy rule without individual authorization; and

3. If a consent for TPO has been/will be obtained, or a notice of privacy practices has been/will be provided, must state that this research authorization is binding.

Options for Research Authorization

Research authorization may be in the same document as:

- The informed consent document;
- A consent to use or disclose PHI to carry out TPO;
- A notice of privacy practices.

Disclosures for research must be accounted for, and revealed to individual when asked.

Individual Access

In general, research participants have a right to access PHI about themselves in designated record sets, except:

- If a covered entity is subject to CLIA and state law prohibits individuals from obtaining access;
- If a covered entity is exempt from CLIA; i.e some research laboratories;
- While a trial is in progress, if the individual has agreed, and has been informed that their right of access will be reinstated at the end of the research.
- If research information is NOT in a DRS.

Designated Record Set

A group of items of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity that is:

- The medical records and billing records about individuals maintained by or for a covered health care provider;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the covered entity to make decisions about individuals.

Definition of Data Aggregation

Data aggregation means the combining of PHI by a business associate with the PHI received from other covered entities, to permit data analyses that relate to the health care operations of the respective covered entities.

Health Care Operations examples

- outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies.
- population-based activities relating to:
  - improving health or reducing health care costs,
  - protocol development,
  - case management and care coordination,
  - contacting of health care providers and patients with information about treatment alternatives.
- evaluating performance of providers and plans.
- training programs.
- accreditation, certification, licensing, or credentialing.

Privacy and Security Regulation Schedule

Final Privacy Rule

- Compliance date April 14, 2003.
- Likely NPRM with modifications “soon.”

Final Security Rule

- Likely publication in Summer 2002.
- Likely compliance date Summer 2004.
- Privacy rule requires some security ‘now’
  - “covered entity must reasonably safeguard PHI.”

Questions?

William.R.Braithwaite@us.PwCglobal.com

http://www.pwchealth.com/hipaa.html

http://aspe.hhs.gov/admnsimp

http://www.hhs.gov/ocr/hipaa