Issues in HIPAA Research Compliance

William R. Braithwaite, MD, PhD
"Dr. HIPAA"

HIPAA Summit 6
Washington, DC
27 March 2003

5 Principles of Fair Info Practices

Notice

- Existence and purpose of record-keeping systems must known.

Choice – information is:

- Collected only with knowledge and permission of subject.
- Used only in ways relevant to the purpose for which the data was collected.
- Disclosed only with permission or overriding legal authority.

Access

- Individual right to see records and assure quality of information.
  - accurate, complete, and timely

Security

- Reasonable safeguards for confidentiality, integrity, and availability of information.

Enforcement

- Violations result in reasonable penalties and mitigation.

The HIPAA Challenge for Researchers

- The Privacy Regulation establishes a stringent new regime that governs all uses and disclosures of PHI.
- Every use and disclosure of PHI by covered entities is prohibited unless specifically permitted or required by the Privacy Rules.

Using PHI for Research Purposes

3 + ways PHI can be used for research:

1. De-identified (or partially de-identified) PHI
   - De-identified by 'safe-harbor' method
   - De-identified by statistical method
   - Limited dataset plus data use agreement
2. PHI without an Authorization
   - PHI with IRB/Privacy Board waiver
   - PHI for research protocol preparation
   - PHI of deceased
3. PHI with authorization of subject

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

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.

1. De-identified Information

De-identified data (under HIPAA) is not PHI.

- Not equivalent to “anonymous” data (under the Common Rule)
- Cannot have any of the following 18 identifiers:

1. Name
2. Geographic subdivisions smaller than State
3. Dates (except year) directly related to patient
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical Record numbers
9. Health plan beneficiary numbers

De-identified Information (continued)

10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers
13. Device identifiers and serial numbers
14. Web URLs
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable image
18. Any other unique identifying number, characteristic, or code except as permitted under HIPAA to re-identify data

- Some useful (derived) elements are still allowed:
  - Age < 90, differences between dates (e.g., LOS), years
  - Gender
  - Most 3-digit zip codes
  - Re-identification code

‘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.

‘Statistical’ De-identification Questions

- Who in the institution will make a determination as to whether data is de-identified?
  - Must be an individual with appropriate knowledge and experience .
- How will the attestation be made to the institution?
- Who in the institution will make the decision regarding de-identified data?
- Does this require a statistician on the Privacy Board or IRB?
- Should the institution consider retaining outside expertise?

Limited Data Set (LDS)

- LDS is protected health information that excludes direct identifiers:
  - Same identifiers must be removed as for de-identified data, except:
    - Full dates
    - Geographic detail of City, State, and 5-digit zip
- Information in LDS cannot be treated or labeled as “de-identified” as it is still PHI protected by HIPAA.

Limited Data Set

- Use of LDS requires a written data use agreement from the recipient that sets conditions.
  - Data use agreement is not a business associate agreement – more specific and targeted.
  - Recipient must agree not to identify or contact the subjects or further disclose the information.
- The minimum necessary provision applies to the limited data set.

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

Permissible under three circumstances:

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

Waiver Criteria

1. Use or disclosure involves no more than minimal risk to individuals' privacy;

- There is an adequate plan to protect the identifiers from improper use and disclosure;
- 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
- 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. Research could not practicably be conducted without the waiver;
3. Research could not practicably be conducted without access to and use of the PHI.

3. Research Use and Disclosure of PHI WITH Individual Authorization

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

- Researchers must comply with all applicable rules.

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

  - May be in same document.

6 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. A description of each purpose of the requested use or disclosure;

6 Core Elements of Authorization

5. An expiration date or an expiration event;
   - Event may be the termination of the research study or "none".
6. Signature of the individual and date;
   - If the authorization is signed by a personal representative, a description of the authority to act for the individual.

3 Statements Required in Authorization

1. A statement of the individual's right to revoke the authorization in writing;
2. The ability or inability to condition treatment on the authorization;
3. The potential for information disclosed pursuant to the authorization to be subject to redisclosure and no longer protected by federal privacy regulations.

Other Authorization Matters

- Authorization must be written in plain language and a copy must be given to the individual.
- If a research subject revokes their authorization, their PHI accumulated to that revocation can continue to be used to maintain integrity of the research.
- Any legal permission received before April 13, 2003 can remain effective until the end of the research project.
  - But if no legal permission has been received, then need to obtain valid authorization by April 13, 2003.
- Subjects enrolled after April 13, 2003 require HIPAA-valid authorization or IRB waiver documentation.

Revocation of Authorization

An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

- The covered entity has taken action based on the authorization; or
- If the authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself.

BUT, CE may continue to use and disclose protected health information obtained prior to the time the authorization was revoked,

- as necessary to maintain the integrity of the research study.

Authorization: Best Route to Research

No Representations (Assurances) Required

No Prior Privacy Board Review

No Accounting of Disclosures Required

No “Minimum Necessary” Limitations

Individual Access

In general, research participants have a right to access and copy PHI about themselves, except:

- If a covered entity is subject to CLIA (special rules apply).
- While a clinical 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 designated record set.

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 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.

Effects of the Final Security Rule

Nothing specific to research …

HOWEVER, privacy rule requires:

- "A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements …"
- "A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures …"

Disclosing Research Data to Others

No disclosures are permitted to others interested in your data unless:

- Mandated by State law
- The authorization permits such disclosures
- The PHI is de-identified
- The PHI is made a limited data set and disclosed under a Data Use Agreement

  or

- A waiver is granted

How do privacy rules affect research?

- New burdens for IRBs.
- Voluntary registries face new hurdles.
- Liability fears may dissuade CEs from sharing data with researchers.
- New forms for research subjects.
- Health Systems must track and account for research disclosures.
- Need for new policies and procedures for handling information
- Need for training

Questions?

William.R.Braithwaite@US.PwCglobal.com