National Committee on Vital and Health Statistics

Workgroup on Secondary Uses of Health Data

Clarity and Intent of HIPAA Privacy Rule on Uses of Health Information

Testimony of
William R. “Bill” Braithwaite, MD, PhD
Health Information Policy Consulting
Washington, DC

July 17, 2007

Principles of Fair Information Practice

- **Notice**
  - Existence and purpose of record-keeping systems must be 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.

HIPAA Uses & Disclosures are Permissive

- Required disclosures are limited to:
  - Disclosures to the individual who is the subject of information.
  - Disclosures to HHS to determine compliance.
- All other uses and disclosures in the Rule are permissive.
- Covered entities can provide greater protections if they want by preventing uses and disclosures that HIPAA allows.

HIPAA Uses & Disclosures are Limited

- Limited to only what is permitted under 4 mechanisms in the Rule:
  1. Treatment, payment, and health care operations (TPO) after notice and acknowledgement.
  2. Uses and disclosures involving the individual's care or directory assistance,
     - Requiring an opportunity to agree or object.
  3. For specific public policy exceptions.
  4. All others as authorized by individual.

- Procedural requirements vary based on type of use or disclosure.

1a. Notice, and Acknowledgement

- Permission to use PHI for TPO is assumed when you go to a health care provider.
  - Provider may obtain written consent, if they wish.
- Notice of Privacy Practices (NPP)
  - Direct treatment provider must provide NPP as soon as reasonably practicable to each new patient.
  - Make a good faith effort to obtain a written acknowledgment.
  - Acknowledgement is not required for:
    - Indirect Treatment Providers,
    - Health Plans,
    - Health Care Clearinghouses.

1b. Health Care Operations

- Examples of Health Care Operations:
  - outcomes evaluation and development of clinical guidelines, **provided that the obtaining of generalizable knowledge is not the primary purpose of any studies (that's research)**.
  - 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.

- Are these Secondary Uses?

2. Opportunity to Agree or Object

- The privacy regulation recognizes the following situations when the individual has the right to agree or object to the use or disclosure of their PHI:
  - Limited information for use in facility directories.
  - Limited disclosures to family members/friends.
  - Disaster relief services.
    - Is this a Secondary Use?

3. Public Policy Exceptions

- Covered entities may use or disclose PHI without a consent or authorization only if the use or disclosure comes within one of the listed exceptions & **certain conditions are met**;
  - As required by law.
  - For public health.
  - For law enforcement.
  - Coroners, medical examiners, funeral directors.
  - ...
  - Health care oversight.
  - For research.
  - Organ transplants.
- Secondary Uses judged ‘for the Public Good’.

4. Authorizations (not TPO)

- Generally, covered entities must obtain an individual's authorization before using or disclosing PHI for purposes other than treatment, payment, or health care operations.
  - Most uses or disclosures of psychotherapy notes also require authorization.
  - Provider marketing and fundraising may require authorization.

- All other Secondary Uses require Authorization!

Business Associates

- A business associate relationship exists when the business associate performs a function that the covered entity could perform for itself.
  - Includes administrative, management, financial services.
  - Generally excludes services requiring licensure.
- EXCEPTION: a BA can perform data aggregation services for TPO that CE could not do for itself
  - because it involves access to PHI from other CEs.

- Secondary Uses outsourced to BAs must follow the same rules.

e.g. Using PHI for Research Purposes

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).

HIPAA Rule of Thumb

- Don’t surprise the patient with a use or disclosure they don’t expect!
  - (or should know to expect)
  1. Tell the patient about all uses and disclosures that are part of normal operations of the healthcare enterprise (TPO).
  2. Give the patient the opportunity to object to limited disclosures in common practice for the good of the patient.
  3. Follow procedure for a public policy exception.
     - e.g., required reporting of contagious disease.
  4. Get explicit permission for anything else.

Conclusions

- Uses and disclosures come in many flavors.
  - Different flavors are treated differently by HIPAA based on principles of fair information practice.
- HIPAA Privacy Rule intent is to protect individual privacy while allowing most current practices to continue with transparency.
  - Most current practices are beneficial but often poorly understood by patients.
- HIPAA Privacy Rule is clear.
  - Complexity of healthcare environment and diversity of desired secondary uses makes it difficult to apply simple rules.

Thank you!

William R. “Bill” Braithwaite, MD, PhD
Washington, DC
bill@braithwaites.com