Health Insurance Portability and Accountability Act Privacy Rule

HIPAA Privacy and the Academic Medical Center

April 21, 2002

Prepared By: Rick Rohrbach
Senior Manager
PricewaterhouseCoopers

Presented By: F. Lisa Murtha
Chief Audit & Compliance Officer
Children’s Hospital of Phila.

The Children’s Hospital of Philadelphia® A pediatric healthcare network
HIPAA Privacy and the Academic Medical Center

HHS perspective on the use and disclosure of Private Health Information in Research

“Covered entities [should] be mindful of the often highly sensitive nature of research information and the impact of individuals’ privacy concerns on their willingness to participate in research.”

Overview

Definitions
Consent and Authorization
Research Implications
Types of Research Covered
Human Subject Regulations vs. HIPAA Privacy Rule
HIPAA Compliance
Final Thoughts
The HIPAA Privacy Prohibition

The HIPAA Privacy Standards generally state that a “covered entity” may not use or disclose protected health information (PHI), except as permitted or required by the regulation.

45 CFR 164.502
Covered Entity
Health plan; Health care clearinghouse; Health care provider that transmits any health information in electronic form.

Individually Identifiable Health Information (IIHI)
Information about the physical or mental health of an individual that is created or received by a covered entity and that identifies or can reasonably be used to identify the individual

Protected Health Information (PHI)
IIHI transmitted or maintained through electronic media
Consent

Consent is a general document that is required for treatment, payment or healthcare operations related uses and disclosures of protected health information.

A covered health care provider must obtain the individual’s written consent prior to using or disclosing protected health information to carry out treatment, payment or healthcare operations.
The following elements must be contained within the consent:

- Written in plain language;
- Inform the individual that PHI may be used or disclosed for treatment, payment or healthcare operations;
- Refer the individual to the covered entity’s notice for additional information, which the individual has a right to view prior to signing the consent;
- Inform the individual of the right to restrict use or disclosure;
- Indicate that the individual has the right to revoke the consent; and
- Indicate individual’s signature and date.

Blue text not included in current IRB informed consent
Authorization

In instances not related to treatment, payment or health care operations, including research, the covered health care provider must obtain the patient’s written authorization, for the use or disclosure of protected health information.
HIPAA Privacy and the Academic Medical Center

The following elements must be contained within the authorization:

- Specific, meaningful description of the information to be used;
- Name, specific id or class of persons authorized to make the requested use or disclosure;
- Name, specific id or class of persons to whom information may be disclosed;
- An expiration date or an expiration event;
- Individual’s right to revoke;
- Statement that information may be subject to re-disclosure;
- Individual’s signature and date
- Description of personal representative is needed if patient is not signing authorization
- Written in Plain language;

For information created for research involving treatment:

- Description of extent to which PHI will be used for treatment, payment or healthcare operations;
- Description of information that will not be used or disclosed as permitted by the rule;
- Refer to the treatment/payment/operations consent and state that the authorization is binding.
Research Implications:

The covered entity does not have to obtain the individual’s consent, or authorization if:

1. The researcher provides assurances for reviews in preparation for research, or
2. The researcher provides assurances for review of decedents information, or
3. Waiver has been approved by the IRB or Privacy Board.
Research Implications:

1. Reviews Preparatory for Research
   In creating research protocols or hypothesis, a covered entity may allow a researcher to use PHI after it obtains representations from the researcher that:
   - use or disclosure is sought solely to review PHI as necessary to prepare for research,
   - no PHI will be removed from the covered entity by the researcher during review, and
   - the PHI is necessary for research purposes only.
Research Implications:

2. Reviews of Decedent Information

A covered entity may allow a researcher to review PHI of deceased individuals, provided the researcher assures that:

- use or disclosure is sought solely to review PHI as necessary to prepare for research,
- no PHI will be removed from the covered entity by the researcher during review, and
- the PHI is necessary for research purposes only, and

The institution may require researcher to provide proof of the individual’s death prior to review.
Research Implications:

3. **IRB or Privacy Board Waiver of Authorization**

A covered entity may rely upon the documented approval of a waiver or alteration of authorization that is given by an Institutional Review Board or a Privacy Board.

The Documentation must include:

- Signature of chair of IRB or PB, or designated member,
- Identification of IRB or PB,
- Identification of the PHI approved for use or disclosure, and
- Specify the review procedures.
HIPAA Privacy and the Academic Medical Center
Criteria for Review of Alteration or Waiver

**IRB Regulations**

**Alter or Waive Informed Consent:**
1. the research involves no more than minimal risk to the subjects;
2. the waiver or alteration will not adversely affect the rights and welfare of the subjects;
3. the research could not practicably be carried out without the waiver or alteration; and
4. Whenever appropriate, the subjects will be provided with additional pertinent information after participation.

**HIPAA**

**Waive or Alter Authorization:**
(A) The use or disclosure of PHI involves no more than minimal risk to the individuals;
(B) The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;
(C) The research could not practicably be conducted without the alteration or waiver;
(D) The research could not practicably be conducted without access to and use of the PHI;

No further criteria.
HIPAA Privacy and the Academic Medical Center
Criteria for Review of Alteration or Waiver

IRB Regulations

Alter or Waive Informed Consent:
No further criteria.

HIPAA

Waive or Alter Authorization:
(G) There is an adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and
(H) There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, 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 this subpart.
HIPAA Privacy and the Academic Medical Center
Review Procedures

**IRB Regulations**

Normal Review: IRB

- A majority of members are present, (an IRB shall have at least 5 members)
- One member whose primary interests are non-scientific
- Approval of a majority of the members present

**HIPAA**

Normal Review: PB

- A convened meeting,
- A majority of the members are present,*
- One member who has no affiliations, and
- Approval of a majority of the members present. *
HIPAA Privacy and the Academic Medical Center
Review Procedures

IRB Regulations

Expedited Review: IRB
• research presents no more than minimal risk to human subjects,
  – on the list of categories
• may be carried out by IRB chair or one or more experienced members as designated by the chair, and
• cannot disapprove research

HIPAA

Expedited Review: PB
• research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI,
• PB must elect to use the expedited review,
• PB chair or one or more of the more experienced members as designated by the chair.
HIPAA Privacy and the Academic Medical Center

An Important Note about Privacy Boards

*Privacy Boards are not Institutional Review Boards*

Privacy Boards exist *only* to perform reviews of the waiver or alteration of an individual’s authorization for the use or disclosure of PHI in research.
Research Implications:

If the 3 conditions are *not* met and PHI is created for research involving treatment of individuals (clinical trials):

- the covered entity must obtain the patient’s consent to use or disclose PHI to carry out treatment and the individual’s authorization to use or disclose PHI created during research.

**Note:** The authorization may be incorporated into the same document as the consent.
Research Implications:

If the 3 conditions are not met and the research does not involve treatment of individuals:

- the covered entity must obtain the patient’s authorization to use or disclose any pre-existing PHI and the individual’s authorization to use or disclose PHI created during research.

There are further authorization requirements for the entity’s own use or disclosure of PHI.
Types of Research covered by HIPAA:

Research that uses existing Protected Health Information -
  Research involving medical records
  Health services research
  Clinical trials
  Research involving tissue specimens with identifiable health information

Research that includes treatment of research participants -
  Clinical trials
# HIPAA Privacy and the Academic Medical Center
## Human Subject Regulations vs. HIPAA Privacy Rule

<table>
<thead>
<tr>
<th><strong>Human Subject Regulations</strong></th>
<th><strong>HIPAA Privacy Rule</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies to <em>federally supported</em> or <em>FDA regulated</em> research</td>
<td>Applies to <em>all</em> research</td>
</tr>
<tr>
<td>Protects <em>rights</em> and welfare</td>
<td>Protects <em>privacy</em> and welfare</td>
</tr>
<tr>
<td><em>Human subject</em>: A living individual about whom an investigator obtains (i) data through intervention/interaction or (ii) identifiable private information; or An individual who participates in research involving a test article</td>
<td><em>Individual</em>: subject of information; a living or deceased person</td>
</tr>
<tr>
<td>Uses Institutional Review Boards (IRBs)</td>
<td>Uses IRBs or Privacy Boards</td>
</tr>
<tr>
<td>Board reviews all non-exempt human subject research</td>
<td>Board reviews only authorization waivers or alterations</td>
</tr>
<tr>
<td>Continuing review at least annually</td>
<td><em>No requirement for continuing review</em></td>
</tr>
<tr>
<td>Informed Consent</td>
<td>Authorization and Consent</td>
</tr>
</tbody>
</table>
HIPAA Compliance - Individual Access to PHI

HIPAA generally recognizes an individual’s right of access to inspect and copy their PHI maintained by a covered entity. Exceptions:

- Psychotherapy notes;
- A covered entity may temporarily suspend/deny access to PHI created for research that involves treatment:
  - while research is in progress,
  - with prior individual agreement, and
  - if the individual is informed that the right will be reinstated at the conclusion of the research.
HIPAA Compliance - Covered Entities and Researchers

Covered entities must obtain written assurances from the person or entity that receives the PHI not to re-use or disclose the PHI.

Exceptions:

- As required by law,
- For authorized oversight of the research, or
- For other research for which the use or disclosure of the PHI would be covered by the regulation.
HIPAA Compliance - Minimum Necessary

Covered entities should obtain assurances from those receiving protected health information including:

- Researchers
- Business Associates
- Others

By obtaining these assurances, the covered entity is deemed in compliance with minimum necessary requirements.
HIPAA Privacy and the Academic Medical Center

HIPAA Compliance - State Law Pre-emption

HIPAA establishes national standards for the use and disclosure of PHI.

HIPAA applies:
- where there is no state law, or
- where state law is more lenient.

HIPAA does not supersede more stringent state laws - i.e. Minnesota Access to Health Records Law, requiring authorization for all medical records research.

ΠωΧ
Final Thoughts

Penalties for Non-Compliance:

Civil:
- $100,000 per incident
- up to $25,000 per person/year/standard
Final Thoughts

Penalties for Non-Compliance:

Federal Criminal:

- up to $50,000 and 1 year in prison for obtaining and disclosing PHI
- up to $100,000 and 5 years in prison for obtaining or disclosing PHI under “false pretenses”
- up to $250,000 and 10 years in prison for obtaining or disclosing PHI with intent to sell, transfer or use for commercial advantage, personal gain or with malicious harm.
Final Thoughts

Compliance Considerations:

- Adopt written privacy policies and procedures
- Designate a Privacy Officer
- Train employees
- Monitor privacy policy compliance
- Establish a grievance procedure
- Take corrective and disciplinary action