Impact of the HIPAA Privacy Rule on Human Subject Research

Impact of the HIPAA Privacy Rule on Human Subject Research

National Audio Conference

February 20, 2003

Michele Russell-Einhorn, JD
202-414-1839
Michele.Russell-Einhorn@us.pwcglobal.com

P w C

Overview

General Rule

Definitions

Permitted disclosures-When not to worry about HIPAA

When to worry about HIPAA

Legally authorized representatives

HIPAA Privacy Rule
In General --

Use or Disclosure of "Protected Health Information" for **research** purposes requires either:

- A written **Authorization** from the subject

  or

- **Verification** that the research involves:
  - => De-Identified Information
  - => Limited Data Sets
  - => Reviews Preparatory to Research
  - => Decedents' Information

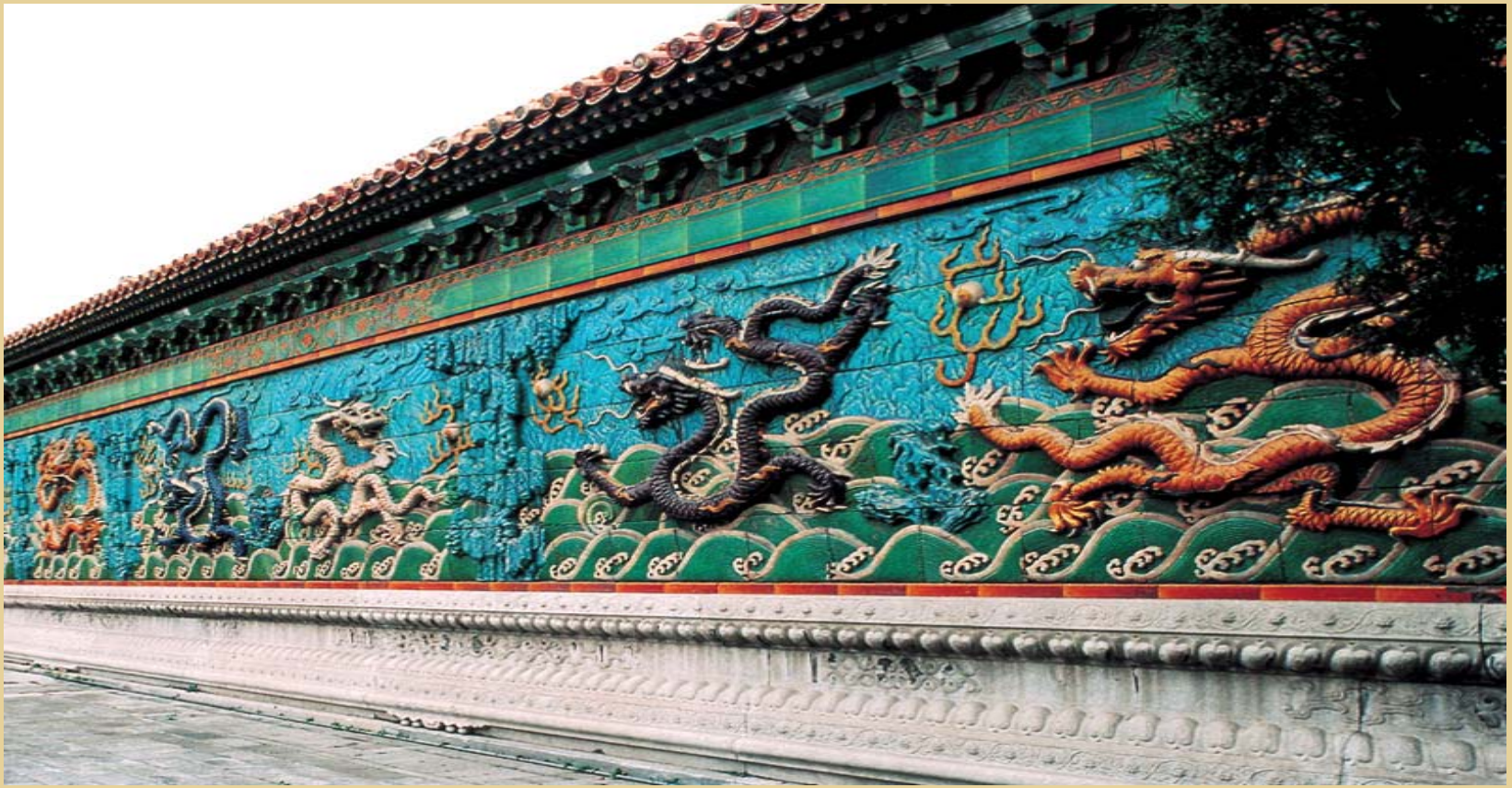
  or

- A **Waiver** approved by the Privacy Board / IRB

Specific Privacy Rule Requirements

P w C

Regulatory Definitions Relating to Research



Definitions

Authorization. Permission from an individual to use or disclose Protected Health Information for a purpose other than Treatment, Payment, or Health Care Operations. A valid authorization must be written in plain language and must include six core elements and three required statements. The individual must be given a signed copy of the authorization that she or he has provided [45 CFR 164.508(c)]. Authorization to use or disclose Protected Health Information for research purposes may be included the research informed consent document.

Business Associate. A person who performs, or assists in performing, a function or activity of a Covered Entity that involves the use or disclosure of individually identifiable health information [§160.103]. Research sponsors and collaborators are not considered Business Associates, unless they also perform a function regulated by the Administrative Simplification Rules, such as such as payment, claims billing, or health care operations.

Covered Entity. A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form [§160.103].

Definitions

Data Use Agreement. An agreement between a Covered Entity and the person or institution that will receive a Limited Data Set. The agreement must state that the recipient will only use or disclose the information in the Limited Data Set for specific, limited purposes [§164.514(e)(4)].

De-Identified Information. Health information that does not identify an individual. Health information can be rendered de-identified either by (i) removal of 18 specified kinds of information about the individual and the individual's relatives, employers, or household members; or (ii) documentation from a professional knowledgeable in statistical and scientific methods that the risk of identification is very small [§164.514(b)]. De-identified information is not subject to the HIPAA privacy requirements [§164.514(a)].

Designated Record Set: A group of records (including any item, collection, or grouping of information that contains Protected Health Information) that is used by or for a Covered Entity to make decisions about individuals. Designated record sets include (but are not limited to) medical records, billing records, health plan enrollment records, payment records, claims records, case management records, and medical management records [§164.501]. Research information that is not related to treatment may or may not be included among the Covered Entity's designated record sets.

Definitions

Disclosure. The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information [§164.501].

Individually Identifiable Health Information. Any information, including demographic information collected from an individual, that:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse.

  and

- Relates to (a) the past, present, or future physical or mental health or condition of an individual; (b) the provision of health care to an individual; or (c) the past, present or future payment for the provision of health care to the individual.

  and

- Identifies the individual or there is a reasonable basis to believe can be used to identify the individual [§160.103].

Definitions

Institutional Review Board (IRB). A committee established to review and approve research involving human subjects in accordance with FDA (21 CFR Part 56) and DHHS Human Subject Protection regulations (45 CFR Part 46). When authorized by the Covered Entity, IRBs may grant waivers of the Privacy Rule's usual requirement for Authorization from the patient-subject for the Use or Disclosure of Protected Health Information in research. Covered Entity's may establish separate Privacy Boards for this purpose, or may delegate this authority to their IRBs [§164.512(i)(1)(i)].

Definitions

Legally Authorized Representative. A personal representative who has the authority under applicable State law to sign an authorization on behalf of another individual. HIPAA requires that a description of the representative's authority to act for the individual must be provided with the authorization [§164.502(g), 164.508(c)(vi)]. :

A parent or legal guardian, if the patient is a minor.

- A legal guardian, if the patient has been found by a court to be incapable of managing the patient's personal affairs.
- An agent of the patient authorized under a medical power of attorney for the purpose of making a health care decision when the patient is incompetent;.
- An attorney *ad litem* and/or guardian *ad litem* appointed for the patient by a court.
- A personal representative or statutory beneficiary, if the patient is deceased.
- An attorney retained by the patient or by the patient's legally authorized representative.
- An attorney-in-fact of the patient.

Definitions

Limited Data Set. Health information that excludes 16 specified kinds of information about the individual and the individual's relatives, employers, or household members. Limited data sets may be used or disclosed for purposes of research under a written Data Use Agreement that satisfies seven specified criteria [§164.514(e)].

Minimum Necessary Standard. A Covered Entity must make reasonable efforts to use, disclose, or request the least amount of information needed for the intended purpose [§164.502(b)]. Relative to research, the Minimum Necessary Standard applies to use or disclosure under (i) a Waiver of Authorization; (ii) Activities Preparatory to Research; (iii) Decedents' Information; and (iv) "Limited Data Sets" (the latter of which also require a Data Use Agreement [§164.514(e)]). The Minimum Necessary Standard does **not** apply to (i) uses or disclosures made under an Authorization, including an Authorization for research [§164.502(b)]; or (ii) Protected Health Information that has been "de-identified [§164.502(d)]."

Definitions

Minor. An individual who has not reached the age at which a person is legally competent or responsible.

Privacy Board. A committee established under HIPAA to grant waivers of the Privacy Rule's usual requirement for Authorization from the patient-subject for the Use or Disclosure of Protected Health Information in research. Covered Entity's may establish separate Privacy Boards for this purpose, or may give this authority to their IRBs [§164.512(i)(1)(i)].

Protected Health Information. Individually identifiable health information that is transmitted or maintained electronically or in any other form or medium, including on paper or orally. Protected Health Information does **not include** education records covered by the Family Educational Rights and Privacy Act and employment records held by a Covered Entity in its role as an employer [§164.501].

Definitions

Psychotherapy Notes. Notes recorded in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the medical record. *Psychotherapy Notes* do not include medication prescription and monitoring; session start and stop times; modalities and frequencies of treatment furnished; results of clinical tests; and any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, or progress [§164.501].

Re-Identification. Use of a code or other means designed to enable coded or otherwise de-identified information to be rendered identifiable. Protected Health Information that is re-identified is subject to the usual HIPAA privacy requirements [§164.502(d)(2)(i),(ii)].

Research. A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge [§164.501].

Use. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information [§164.501].

Definitions: Regarding Research Partners

Business Associates

- Must do something other than research “on behalf of” the covered entity
- Research sponsors and collaborators are not considered Business Associates, unless they also perform a function regulated by the Administrative Simplification Rules, such as such as payment, claims billing, or health care operations
- When a pharmaceutical company hires an investigator to conduct research, it is not doing something on behalf of the university. Thus, the PI would not have to enter into a BAA with a pharmaceutical company.

Protected Health Information

PHI is individually identifiable health information that is:

- Transmitted by electronic media, *or*
- Maintained in any medium described in the definition of electronic media at Section 162.103 of this subchapter, *or*
- Transmitted or maintained in **any other form or medium**

Except for:

- Education records covered by the Family Educational Rights and Privacy Act
- Employment records held by a Covered Entity in its role as an employer [§164.501]

When NOT to Worry About HIPAA Requirements!

PricewaterhouseCoopers

Permitted Disclosures Applicable to Research

Permitted Disclosures for Public Health Activities (164.512)

- To a public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions (e.g, cancer registries, incidents of West Nile)

or

- At the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.

Permitted Disclosures Applicable to Research

NOTE:

A public health activity is not disclosure to a data base or a repository, unless such is required by law.

- Tissue banking for DNA research

Permitted Disclosures Applicable to Research

- Reporting of child abuse or neglect, other abuse or neglect, or domestic violence.
- Informing a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation;

Permitted Disclosures Applicable to Research

- To persons subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:
  - To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
  - To track FDA-regulated products;
  - To enable product recalls, repairs, or replacement…
  - To conduct post-marketing surveillance

Permitted Disclosures
Health Oversight Activities

- To a **health oversight agency** for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions, or other activities necessary for appropriate oversight of:
  - (iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards;

Permitted Disclosures
Health Oversight Activities

Who is considered a Health Oversight Agency?

Does this section permit disclosures to:

- ✓ OHRP
- ✓ FDA
- Your Institution's IRB
- An independent IRB
- The sponsor (164.512(b)(1)(iii))
- An institutional audit committee

Permitted Disclosures vs. Certificates of Confidentiality

A covered entity may disclose PHI for judicial or administrative proceedings expressly authorized by a court or tribunal order or in response to a subpoena, discovery request or lawful process if:

- Satisfactory assurances have been given that reasonable efforts have been made to notify the individual *or*
- Reasonable efforts have been made to secure a protective order

Permitted Disclosures vs. Certificates of Confidentiality

- Can a Certificate of Confidentiality trump the disclosure provisions in 164.512 (e)?
  - The disclosure provisions in 164.512 are not absolute and provide the covered entity with much discretion.
- The Certificate of Confidentiality derives from an HHS statute 42 USC Section 241(d).
  - This would likely over-ride the HHS HIPAA regulations.
  - Alternatively, a court could read the two together so that they would be as consistent with each other as possible.

What Does HIPAA Require When Use and Disclosure Are Not Permitted?

PricewaterhouseCoopers

Notice of Privacy Practices

All research subjects must receive a Notice of the Covered Entity's Privacy Practices.

- Clearly posted at institution
- Available upon request of patient-subject
- Paper copy provided to research subject
- A Notice of Privacy Practices (NOPP) is subject to specific regulatory content requirements.

Authorization

Generally, uses and disclosures of protected health information in research must be conducted pursuant to a valid **Authorization….**

- 6 Core elements
- 3 Required statements
- 2 Additional requirements

Authorizations

1. Authorization for Use and Disclosure of Protected Health Information in Research CAN be combined with an informed consent document.
2. An Authorization for Use and Disclosure of **Psychotherapy Notes** in Research CANNOT be combined with any other Authorization or informed consent.
3. Participation in research CAN be condition on an individual signing an Authorization.

Authorization = Most Advantageous Route to Research

- No Representations (Assurances) Required
- No Privacy Board Review Required
- No Accounting of Disclosures Required
- No “Minimum Necessary” Limitations

Use and Disclosure of Protected Health Information without an Authorization

Use and Disclosure of Protected Health Information without an Authorization

5 Ways to Get Protected Health Information for Research without Authorization:

1. Waiver of Authorization Requirements
2. Use of De-identified Information
3. Use of Limited Data Sets
4. Research on Decedents' Information
5. Reviews Preparatory to Research

Research without Authorization: 1. IRB Waiver vs. HIPAA Waiver

IRB Waiver

1. **The research involves no more than minimal risk to subjects;**

HIPAA Waiver

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

- **-- Plan to prevent inappropriate use or disclosure**
- **-- Plan to destroy**
- **-- Written Assurance not to Use or Disclose inappropriately**

Research without Authorization: 1. IRB Waiver vs. HIPAA Waiver

IRB Waiver

2. **The waiver or alteration will not adversely affect the rights and welfare of the subjects;**

HIPAA Waiver

No Comparable Element

Research without Authorization: 1. IRB Waiver vs. HIPAA Waiver

IRB Waiver

3. **The research could not practicably be carried out without the waiver or alteration; and**

HIPAA Waiver

(B) The research could not practicably be conducted without the waiver or alteration;

and

(C) The research could not practicably be conducted without access to and use of the protected health information.

Research without Authorization: 1. IRB Waiver vs. HIPAA Waiver

IRB Waiver

4. **Whenever appropriate, the subjects will be provided with additional pertinent information after participation.**

HIPAA Waiver

No Comparable Element

Research without Authorization: 1. Documentation of HIPAA Waiver

1. Identification and date of action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;
2. Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the waiver criteria.
3. A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined…

Research without Authorization: 1. Documentation of HIPAA Waiver

4. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures …
5. Signature of IRB Chair or other member of IRB or Privacy Board.

Research without Authorization: 2. De-identified Information

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. (164.514(a))

- De-identification may be achieved through:
  - Statistical Determination

    or
  - Removal of Specific Identifiers

Research without Authorization: 2. De-identified by Statistical Expert

Information is de-identified only if:

(1) A person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rending information not individually identifiable:

- (i) Applying such principles and methods, 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 who is a subject of the information;

  and

- (ii) Documents the methods and results of the analysis that justify such determination;

Research without Authorization: 2. De-identified by Statistical Expert

- Who in the institution will make a determination as to whether data is de-identified?
- Must be an individual with appropriate expertise.
- 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?

Research without Authorization: 2. De-identified by Removal of Identifiers

Information is de-identified only if:

(1) … *or*

(2)(i)The following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

(A) Names;

Research without Authorization: 2. De-identified by Removal of Identifiers

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

Research without Authorization: 2. De-identified by Removal of Identifiers

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

Research without Authorization: 2. De-identified by Removal of Identifiers

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle Identifiers and serial numbers, including license plate numbers;

Research without Authorization: 2. De-identified by Removal of Identifiers

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs)

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images;

and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section;

and

Research without Authorization: 2. De-identified by Removal of Identifiers

and

(2)(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Research without Authorization: 2. De-identified Information May Include

- Gender
- Age Under 90
- Codes for Re-identifying the Information

Research without Authorization: 2. Re-identification of De-identified Info

A covered entity may assign a code or other means of record identification to allow de-identified information to be re-identified by the covered entity provided that:

(1) Derivation: The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; (*meaning: you can't use the ss # or address or date of birth as the code for re-identification*)
and

(2) Security: The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

Research without Authorization: 2. De-identified Information

A CE may use Protected Health Information (PHI):

- To create De-identified Information that will be disclosed to a Business Associate

  or

- To disclose to a Business Associate where the Business Associate will be de-identifying the PHI. (164.502(d)(1)

Research without Authorization: 3. Limited Data Sets

Criteria for Use:

- Limited data set meeting regulatory requirements for removal of specific identifiers
- Data set recipient
- Data Use Agreement

Research without Authorization: 3. Limited Data Sets

The Limited Data Set May **NOT** include:

(i) Names

(ii) Postal address information, other than town or city, state, or 5-digit zip code (Note: LIMITED DATA SETS can include city, state, and 5-digit zip code but DE-IDENTIFIED information cannot)

(iii) Telephone Numbers

(iv) Fax numbers

(v) Electronic mail address

Research without Authorization: 3. Limited Data Sets

The Limited Data Set May **NOT** include:

(vi) Social security numbers

(vii) Medical record numbers

(viii) Health plan beneficiary numbers

(ix) Account numbers

(x) Certificate/license numbers

(xi) Vehicle identifiers or serial numbers, including license plate numbers

Research without Authorization: 3. Limited Data Sets

The Limited Data Set May **NOT** include:

(xii) Device identifiers or serial numbers

(xiii) Web Universal Resource Locators (URLs)

(xiv) Internet Protocol (IP) addresses

(xv) Biometric identifiers, including finger and voice prints

or

(xvi) Full face photographic images or any comparable images.

Research without Authorization: 3. Limited Data Sets

The Limited Data Set **MAY** include:

- City, state, and 5-digit zip code
- Dates

Research without Authorization: 3. Limited Data Sets

- The Data Use Agreement must state that the limited data set recipient will only use or disclose the protected health information for limited purposes.
- The Data Use Agreement must meet certain content requirements.

Research without Authorization: 4. Research on Decedents' Information

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

ISSUE: What if the information about the decedent is identifiable back to living individuals and affects their individually identifiable health information?

Research without Authorization
5. Reviews Preparatory to Research

(A) Representation (assurance) by the investigator to the covered entity that the use or disclosure is being sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes "preparatory to research."

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

Research without Authorization
5. Reviews Preparatory to Research

- Could information be recorded with identifiers?
  - Yes, ***but*** the information may not be removed from the Covered Entity at any time
    and
  - Human Subject IRB approval would be required

Research without Authorization
5. Reviews Preparatory to Research

- Could a Review Preparatory to Research be used to identify potential research subjects?
  - Yes
- Could a Review Preparatory to Research be used to recruit / contact prospective research subjects?
  - Yes, ***But***
  - Only by members of the covered entity's workforce
  - Human Subject IRB Approval would be required
  - Many covered entity's have decided not to permit recruitment under Reviews Preparatory to Research and will require a Waiver of Authorization instead

Research without Authorization
5. Reviews Preparatory to Research

- Who can perform a Review Preparatory to Research?
  - A member of the Covered Entity's workforce who has provided the required Representation (Assurance)

Research without Authorization
5. Reviews Preparatory to Research

- Could a Review Preparatory to Research be used by researchers who are not members of the Covered Entity's workforce?
  - **Possibly, *if***
  - The covered entity permits access
  - Appropriate Representation/Authorization is provided
  - Protected Health Information is not removed from the covered entity
  - Protected Health Information is not used to contact prospective subjects

Other Regulatory Issues…

Consent or Authorization From Someone Other than the Subject

- Under the Common Rule, informed consent is to be obtained from the subject or the subject's Legally Authorized Representative (LAR)
  - Some institutional attorney's have interpreted State statutes authorizing surrogates to consent in medical situations as capable in research situations as well.
- The Privacy Rule requires that *a description of the LAR's authority to act for the individual be provided with the authorization* [§164.502(g), 64.508(c)(vi)].

Consent or Authorization From Someone Other than the Subject

Informed Consent:

- Signed by a Legally Authorized Representative (LAR)

Authorization:

- Signed by a Legally Authorized Representative (LAR)
- With a description attached of the authority of that person to serve as the Legally Authorized Representative (LAR)

Psychotherapy Notes

Psychotherapy Notes are notes that:

- Are recorded in any medium by a health care provider who is a mental health professional

  and

- Document or analyze the contents of conversation during a private counseling session or a group, joint, or family counseling session

  and

- Are separated from the rest of the medical record

Psychotherapy Notes

Psychotherapy Notes do NOT include:

- Medication prescription and monitoring
- Session start and stop times
- Modalities and frequencies of treatment furnished
- Results of clinical tests
- Any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, or progress [§164.501].

Psychotherapy Notes Authorization and Research Consent

An Authorization for the Use and Disclosure of Psychotherapy Notes

- May **NOT** be combined with Informed Consent for Research
- May **ONLY** be combined with another Authorization for use or disclosure of Psychotherapy Notes

Research Begun Prior to April 14, 2003

- Uses and disclosures pursuant to a valid informed consent obtained from subjects prior to April 14, 2003 may continue without additional Authorization.
  - Includes information obtained before or after April 14, 2003.
- Uses and disclosures pursuant to an appropriate waiver of informed consent for subjects prior to April 14, 2003 may continue without additional Authorization.
- Uses and disclosures for subjects enrolled on or after April 14, 2003 require valid Authorization, Waiver, etc.

Research Begun Prior to April 14, 2003

- What about research that begins before April 14, 2003, but continues to enroll new subjects after April 14, 2003?
- Subjects enrolled after April 14, 2003 must sign an Authorization for Use and Disclosure of Protected Health Information in Research
  - Option 1: Revise Informed Consent Document to include Research Authorization (Requires new IRB Review)
  - Option 2: Continue to use Approved Informed Consent Document and add a separate Authorization Document (Does NOT require new IRB Review)

Penalties for Violations Under Section 262 of HIPAA Statute

Civil Penalties:

- $100 per violation
- Capped at $25,000 for each year
- Enforced by HHS, Office of Civil Rights

Criminal Penalties:

- Knowing violations
- Enforced by Dept. of Justice

Authorization = Most Advantageous Route to Research

- No Representations (Assurances) Required
- No Prior Privacy Board Review
- No Accounting of Disclosures Required
- No “Minimum Necessary” Limitations

Institutional Decisions

P w C

Institutional Issues

- Which office/department finances HIPAA compliance?
- Who enforces Privacy Rule Policies?
- Who makes Privacy Rule determinations?
- Who is responsible for Privacy Rule training?
- Who maintains documentation?
- Who tracks Disclosures?
- Who follows up on requests for accountings?

Institutional Organizational Structure

- Privacy Official
- Privacy Complaint and Contact Official
- Research Privacy Officer
- Research Privacy Monitoring Board
- Privacy Board vs IRB

The Privacy Board Process

- Can expedite only if it determines that a waiver or alteration is appropriate.
- Must meet in a convened meeting if the request for a waiver or alteration will be disapproved.

Impact on Investigators

P w C

Research using Medical Records

HIPAA Privacy Rule

- Review preparatory to research.
- Research done pursuant to a HIPAA waiver.
- Research done under an authorization.
- Decedents' information.

Common Rule

- Research might be exempt or expeditable

Multi-Center Trials

Should be set out in Authorization:

- Communication to co-investigators.
- Receipt of information on adverse events from other sites.
- NOTE: Collaborators are not considered Business Associates unless they also perform functions like payment, claims billing, or health care operations on behalf of the covered entity

Disclosing Information to Others Interested in Your Data

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

Other issues

Accounting for disclosures

Individual access

Suspension of right of access

Designated record sets

Minimum necessary

Revocation of authorizations

Effect of the new security rule

Accounting for Disclosures

On demand by individual, account for all disclosures in past 6 years -

Except **[most]** disclosures: -

- For treatment, payment and health care operations purposes
- To the individual
- Incident to a use or disclosure otherwise permitted or required
- Pursuant to an authorization
- In a facility's directory or to persons involved in the individual's care
- For national security or intelligence purposes
- To correctional institutions or law enforcement officials
- As part of a limited data set
- That occurred prior to the compliance date

Account for these Disclosures

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

- (a) uses and disclosures required by law.
- (b) uses and disclosures for public health activities.
- (c) disclosures about victims of abuse, neglect or domestic violence.
- (d) uses and disclosures for health oversight activities.
  - Subject to temporary suspension.
- (e) disclosures for judicial and administrative proceedings.
- (f) disclosures for law enforcement purposes.
  - Subject to temporary suspension.
- (g) uses and disclosures about decedents.
- (h) uses and disclosures for cadaveric organ, eye or tissue donation purposes.
- (i) uses and disclosures for research purposes.
- (j) uses and disclosures to avert a serious threat to health or safety.
- (k) uses and disclosures for specialized government functions, **except**:
  - National security and intelligence activities, and
  - Correctional institutions and other law enforcement custodial situations.
- (l) disclosures for workers' compensation.

Individual Access

individual has a right to inspect and obtain a copy of PHI about them in a designated record set, for as long as the PHI is maintained in the designated record set, except for:

- (i) Psychotherapy notes;
- (ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
- (iii) Protected health information maintained by a covered entity that is prohibited by law to be given to the individual
  - subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA)

Other exceptions provide reviewable and unreviewable grounds for denial

Suspension of Right of Access

Unreviewable grounds for denial of access include:

- access to protected health information created or obtained in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress,
- provided that the individual has agreed to the denial of access when consenting to participate in the research, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

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.

[Note that research information not used to make decisions about the individual subjects may be left out of the DRS.]

Minimum Necessary

Covered entities must make reasonable efforts to limit the use or disclosure of PHI to minimum amount necessary to accomplish their purpose.

Exceptions:

- Disclosure to or request by provider for treatment.
- Disclosure to individual.
- Under authorization (unless requested by CE).
- Required for HIPAA standard transaction.
- Required for enforcement.
- Required by law.

Revocation of authorizations

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

- (i) The covered entity has taken action in reliance thereon; or
- (ii) If the authorization was obtained as a condition of obtaining insurance coverage, 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.

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 of this subpart.”
- “A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.”

P w C

Your worlds Our people