Health Insurance Portability and Accountability Act (HIPAA) Regulations and Research Projects

Ada Sue Selwitz, M.A.
Director, Office of Research Integrity
Adjunct Associate Professor, Behavioral Sciences
Co-Director, CCTS Regulatory Support
University of Kentucky
February 2014

Acknowledgements

- Joe Brown, University of Kentucky
- Jennifer Hill, University of Kentucky
- Julie Kaneshiro, Office for Human Research Protections (OHRP)
- Dan Nelson, University of North Carolina
- Pearl O'Rourke, Partners Health Care, Boston, Massachusetts
- Carol J. Weil, National Cancer Institute

Examples of Regulations Impacting Privacy/Confidently in Human Research

- Institutional Review Board (IRB)
  - 45 CFR 46; Common Rule; FDA; 21 CFR 50 & 56
- U.S. Department of Education – Family Educational Rights and Privacy Act (FERPA) – Student Records
- U.S. Department of Justice – Privacy Certificates
- National Institutes of Health (NIH) Confidentiality Certificate

Examples of Regulations Impacting Privacy/Confidently in Human Research Continued

- Health Information Technology for Economic and Clinical Health (HITECH) – Office of Civil Rights
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Office of Civil Rights

Ground Rules – HIPAA/HITECH

- Be Gentle – I Do Not Have All of the Answers
- The Answer May be It "Depends"
- Do Not Blame Me – I Didn't Write It!

What is HIPAA?
DHHS/Office for Civil Rights

- Health Insurance Portability and Accountability Act of 1996
- Effective April 2003

What is HIPAA?

- A Lengthy and Complex Statute
- Authorizes Multiple Regulations: (e.g., Security, Transactions & Code Sets, Privacy)
- Focus on Privacy Issues

HIPAA *NOT* a research regulation

- Real Aim Was to Safeguard the Privacy of Medical Information and Prevent Insurance Discrimination and Identity Theft
- HIPAA Recognizes That the Research Community has Legitimate Need for PHI and Includes Some Research Permissions
- Does Include Some Research Specific Requirements

Carol J Weil, National Cancer Institute

What is HITECH?

- Health Information Technology for Economic and Clinical Health Act 2009
- Part of American Recovery & Reinvestment Act 2009
- Designed to Promote Adoption & Standardization of Health Information Technology
- Required HHS to Modify HIPAA's Privacy, Security, & Enforcement Rules

Recent Modifications

- DEPARTMENT OF HEALTH AND HUMAN SERVICES 45 CFR Parts 160 and 164 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, January 17, 2013 http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- Department of Health and Human Services (DHHS) CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports Jointly released by Centers for Medicare & Medicaid Services (CMS), the Centers for Disease Control and Prevention (CDC), and the Office for Civil Rights (OCR), February 3, 2014 https://www.federalregister.gov/articles/2014/02/06/2014-02280/clia-program-and-hipaa-privacy-rule-patients-access-to-test-reports

Security/Breaches of Notification/Enforcement: HITECH

- Strengthen Requirements to Report Breaches
- New Civil Monetary Penalties
- Extension of Enforcement to Business Associate Agreements
- Compound Authorizations
- Compound Authorizations – Future Research

Objectives

1. To Provide an Overview of HIPAA Privacy Requirements That Impact Research
2. To Discuss How HIPAA Differs From Human Research Protection (i.e. IRB) Regulations
3. To Share a Select List of Frequently Asked Questions Regarding Research & HIPAA

How Does the Privacy Rule Affect MY Research?

Depends on:

Who You Are/Where You Work

Type of Information You Use, Collect, or Release

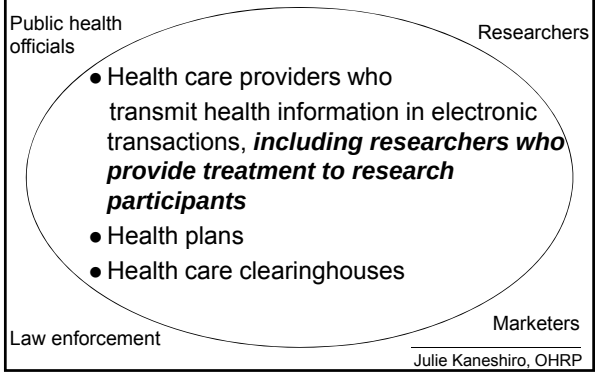
Objective 1: HIPAA Privacy Overview

1. Does HIPAA Apply to Your Research?
2. How Do You Access Data or Share Data Under HIPAA for Research Purposes?
3. What Rights Do the Patient/Subject Have and How Do Those Rights Impact Your Research?
4. Are There Additional Requirements That Impact Research?
5. How Long Must HIPAA Records be Retained?
6. What Penalties Can be Applied if You Do Not Comply With HIPAA Requirements?

When Does HIPAA Apply to Your Research?

Applicability

Who is Covered?



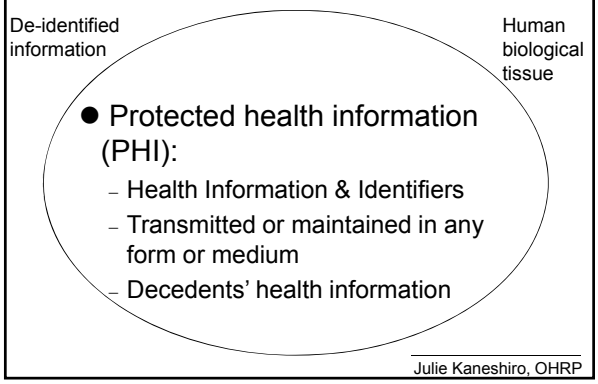
Julie Kaneshiro, OHRP

Types of Covered Entities*

- Free Standing, Single Entity (e.g. Community-Based Hospital)
- Hybrid Entity (e.g. University of Kentucky)
- Affiliated Covered Entity (ACE)
- Organized Health Care Arrangement (OHCA)

*Healthcare Provisions, Clearinghouses, Health Plans

What is Covered?



Julie Kaneshiro, OHRP

Protected Health Information (PHI)

- Individually Identifiable Health Information That a Covered Entity Creates or Receives
  - Includes Information About:
    - The Past, Present or Future Physical or Mental Health of a Person;
    - The Provision of Healthcare to a Person; and
    - Payment for Care
  - Includes Information in Written, Electronic or Oral Form

What is an Identifier in the Privacy Rule?

The Privacy Rule defines 18 identifiers

- Names (Initials)
- Geographic info (including city, state, and zip)
- Elements of dates*
- Telephone #s
- Fax #s
- E-mail address
- Social Security #
- Medical record, prescription #s
- Health plan beneficiary #s
- Account #s
- Certificate/license #s
- VIN and Serial #s, license plate #s
- Device identifiers, serial #s
- Web URLs
- IP address #s
- Biometric identifiers (finger prints)
- Full face, comparable photo images
- Unique identifying #s

*Can Release Age But Not Birthdate

When Does HIPAA Apply to Your Research?

- If the PHI are Held by a Covered Entity

AND

- If Any of 18 Identifiers are Included with the PHI

HIPAA Applies!!!

Case Study

Dr. Doright Collects the Following Data: Birthday, Whether They Smoke, What Medicine They Take From Individuals That He Recruits From the Local Mall.

Is the Research HIPAA Regulated?

Researchers

- Must Know Whether You Are “In” or “Outside” of the Covered Entity and
- Must Recognize “Protected Health Information”

HIPAA Research Rules Differ Based Upon Whether You Are In or Out of the Covered Entity

- Researchers: If You are Collecting PHI from a Covered Entity and You are Not in the Covered Entity, What Must You Do?
- Find Out How that Covered Entity Handles HIPAA in Research

Please Be Aware That the Privacy Rule is Open to Much Interpretation and Every Institution Decides How Best to Implement This Rule in the Context of Other Local/Institutional Policies.

Joe Brown, University of Kentucky

Applicability
What is Not Covered Under HIPAA?

De-identified Health Information

De-identified Health Information – 2 Options

1. All 18 Identifiers Removed
2. Statistically "De-identified" Information: Statistician Certifies "Very Small" Risk That Information Could Identify the Individual

De-Identification Involves Removing These Identifiers:

- Names (Individual, Employer, Relatives, Initials)
- Address (Street, City, County, Zip Code - More than 3 Digits, or Any Other Geographical Codes)
- Telephone/Fax Numbers
- Social Security Numbers
- Dates (Except for Years)
  - Birth Date
  - Admission Date
  - Discharge Date
  - Date Of Death
- All Ages > 89 and All Elements of Dates Indicative of Such Age (Except that Such Age and Elements May be Aggregated Into a Category "Age > 90"
- E-mail Addresses/URLs
- Medical Record Numbers
- Health Plan Beneficiary Numbers
- Account Numbers
- Certificate/License Numbers
- Vehicle Identifiers and Serial Numbers (e.g. VINs, License Plate Numbers)
- Device Identifiers and Serial Numbers
- Biometric Identifiers (e.g. Finger or Voice Prints) or Photographs
- Any Other Unique Identifying Number, Characteristic, or Code

Identifiers that May be Used and Data Will Still be Considered De-Identified:

- Race
- Age (89 or younger) (years – not dates)
- Gender

Joe Brown, University of Kentucky

Case Study

Dr. Doright Receives Data from Dr. X for His Epidemiology Study on Cancer in Lexington, KY. Dr. Doright Receives the Following Data from Dr.X:

- Date of Birth
- Type of Cancer
- Stage
- Year of Diagnosis
- Year of Death (if Applicable)
- Race
- Urban vs Rural Dwelling
- Zip code
- Education
- Median Income

Case Study (Continued)

- Are the Data De-Identified/ Anonymous According to the HIPAA Regulations. Why/Why Not?

Case Study

- Dr. Doright is Getting the Following Data from the Pathology Department: Specimens – Fresh; Tumor Type/ Location; Diagnosis; Smoking History; Age; Gender; Subject Number (Which is the Medical Record Number).
- Dr. Doright Stores the Specimens Separate from the Subject Number so He Does Not Know the Identity of Subjects But He has Access to the Code.
- Do HIPAA Rules Apply?

Code Links

- The Privacy Rule Does NOT Apply to De-identified Information But
- Privacy Rule Does Apply to the Code (Link) That Allows Identification of Coded Information

Pearl O'Rourke
Partners Health Care

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
National Institutes of Health

NIH Research Repositories, Databases, and the HIPAA Privacy Rule
Frequently Asked Questions & Answers

1. A researcher requests data that assigns a code derived from the last four digits of the social security number. This code is necessary to link individual records from different data sources. The data contain none of the other listed HIPAA identifiers at section 164.514(b)(2). Are the data de-identified under the Privacy Rule?

   No. Under the Privacy Rule, a de-identified data set may not contain unique identifying codes, except for codes that have not been derived from or do not relate to information about the individual and that cannot be translated so as to identify the individual. A code derived from part of a social security number, medical record number, or other identifier does not meet this test.

Can a Researcher De-Identify the Data?

- If the Researcher Is In the Covered Entity…
  - Yes Researcher Can De-Identify Data (Under Operations)
- If Researcher is Employed Outside of Covered Entity…
  - Business Associate Agreement Required Before the Researcher can De-identify the Data (Check with the CE)

How Do Researchers Access Information?

Access & Sharing

How do Researchers Access Patient Information? 5 HIPAA Options

1. Written Authorization From Subject
2. IRB/Privacy Board (PB) Waiver of Authorization
3. Preparatory Work (3 Conditions)
4. Decedent Data (3 Conditions)
5. Limited Data Set Which Requires a Data Use Agreement

* Business Associate Agreements May be Required

How Do Researchers Share PHI With Colleagues/Sponsors/ Regulatory Agencies?

How Do Researchers Share PHI? 7 Options

1. Written Authorization From Subject
2. IRB/PB Waiver of Authorization
3. Preparatory Work (3 Conditions)
4. Decedent Data (3 Conditions
5. Limited Data Set Which Requires a Data Use Agreement
6. Required By Law*
7. For Public Health Activities*

*Will Not Discuss Today

If You Are In CE & If You Plan to Share PHI…

- Check Authorization/Re-Authorize, if Needed
- If No Authorization, Can Only Share by Using Options
- Set Up Procedures to Meet Option Requirements

5 HIPAA Options for Accessing or Sharing

1. Authorization
2. IRB/Privacy Board (PB) Waiver
3. Preparatory Work
4. Decedent Data
5. Limited Data Set/Data Use Agreement

Two Terms That Have Special Meaning Under HIPAA For Research

- "Use" - Sharing Within the Entity
- "Disclosure" – Sharing Outside the Entity

6 Core Elements Must Be Included In Authorization

1. Specific Description of Information to be Used/Disclosed
2. Identification of Person or Class of Persons/Authorized to Make Disclosure/Use
3. Identification of Person or Class of Persons to Whom Covered Entity (CE) Releases the Information

6 Core Elements Must Be Included In Authorization (Cont.)

4. Description of Each Purpose of the Requested Use or Disclosure (Why Use or Disclosure is Being Made)
5. Expiration Date Related to Purpose of the Use/Disclosure (Can be Indefinite)
6. Signature of Individual & Date [If Personal Representative, Description of Authority to Act for Individual]

164.508(c)(1)(i-vi) See Example Template

Authorization: Required Statements

- Statement that the Information May be Disclosed to Others Not Subject to the Privacy Rule
- Statement that the Covered Entity May or May Not Condition Treatment or Payment Based on the Individual's Agreement to Sign the Authorization
- Potential for Information to be Subject to Re-Disclosure
- Individual's Right to Revoke Authorization in Writing

164.508(c)(2)(i-iii) See Example Template

Authorization: Additional Statement Researchers May Include

- Subject has a Right to Access Their PHI
- Researchers Can Include in the Authorization a Statement that Tells Subjects That They Cannot Access Their PHI Until the Research is Completed

JOHNS HOPKINS MEDICINE

Frequently Asked Question

I am enrolling subjects in a clinical study. If adverse events occur and my subjects are treated by a provider outside of my Covered Entity, how may I obtain information about the subjects' treatment?

A subject must sign an Authorization that allows the other provider to disclose PHI to you for the purposes of research involving that subject. It is helpful to obtain the subject's express permission for such a disclosure in the Authorization form that the subject signs for your research study. The other provider may rely upon such Authorization; alternatively, the provider may ask the patient to sign the provider's own Authorization, or may disclose the records directly to the patient.

Must Authorization Forms be Reviewed & Approved by an IRB?

- IRB Review of Form Not Required by HIPAA
- But CE May Require that an IRB Review the Authorization Form

2013 Modification to HIPAA

- Compound Authorization Which Allows Researchers to Combine Authorizations With Informed Consents or …

Compound Authorizations - 2013

(3) *Compound Authorizations*. An Authorization for Use and Disclosure of Protected Health Information May Not Be Combined With Any Other Document to Create a Compound Authorization, Except as Follows: (i) An Authorization for the Use or Disclosure of Protected Health Information for a Research Study May Be Combined With Any Other Type of Written Permission for the Same *or Another* Research Study. "*This Exception Includes Combining an Authorization for the Use or Disclosure of Protected Health Information for a Research Study With Another Authorization for the Same Research Study, With an Authorization for the Creation or Maintenance of a Research Database or Repository, or With a Consent to Participate in Research…[.]*"

[New] 45 CFR §164.508(c)(3)(i) (Emphasis Added)

Compound Authorizations - 2013

Where a Covered Health Care Provider has Conditioned the Provision of *Research-Related Treatment* on Provision of One of the Authorizations…Any Compound Authorization Created Under This Paragraph Must *Clearly Differentiate Between the Conditioned and Unconditioned Components* and Provide the Individual With an Opportunity to *Opt-In* to the Research Activities Described in the Unconditional Authorization.

[New] 45 CFR §164.508(c)(3)(iii)

Example:

- Conditioned Component: Subject Must Agree to Use of PHI to Participate in the Study
- Unconditioned Component: Subject Can Participate in the Study and Still Say No to Use/Disclosure of PHI for This Part of the Study! (e.g. Repository)

Compound Authorization – 2013 Modification: Lay Language

- The PI is Enrolling a Subject for a Clinical Trial and a Banking Sub-Study
- Under Recent Modifications, Researchers can Combine the Main Study and Sub-Study in One Authorization (Compound Authorization Form)
- The Clinical Trial is Called the "Conditional Component" and the Optional Sub-Study is the "Unconditional Component"
- Researcher can't Tell Subjects that They Must Participate in the Sub-Study (Unconditional Component) in Order to Participate in the Clinical Trial (Conditional Component)
- It Should be Clear in the Authorization Form

Joe Brown, University of Kentucky

Compound Authorizations – 2013: Notes

1. *The New Expansion is Not Limited to Combining Authorization for a Research Study With an Authorization for a Research Database or Repository; the Expansion Applies to Combinations of Authorizations for Any Types of Research Studies.*

Fred Hamilton, JD, Sinai Medical Center of Florida

Compound Authorizations – 2013: Notes

3. A Combined Authorization Which Permits an Individual Only to Opt Out of an Unconditioned Research Activity is Not Permitted.

   "We Decline to Permit a Combined Authorization That Only Allows the Individual to Opt Out of the Unconditioned Research Activities (e.g. 'Check Here If You Do NOT Want Your Data Provided to the Biospecimen Bank') Because an Opt-Out Option Does Not Provide Individuals With a Clear Ability to Authorize the Optional Research Activity, and May Be Viewed as Coercive by Individuals."

Fred Hamilton, JD, Sinai Medical Center of Florida

More…2013 Modification to HIPAA

- New Modifications Allow Researchers to Obtain Authorization for Future Uses Under Certain Conditions
- This Change Helps Researchers Who Want to Establish Repositories for Future Research

Approvability of Compound Authorization for Future Research

"In Order to Satisfy the Requirement That an Authorization Include a Description of Each Purpose of the Requested Use or Disclosure, an Authorization for Uses and Disclosures of Protected Health Information *for Future Research Purposes* Must Adequately Describe Such Purposes Such That It Would Be Reasonable for the Individual to Expect That His or Her Protected Health Information Could Be Used or Disclosed for Such Future Research."

Fred Hamilton, JD, Sinai Medical Center of Florida

Approvability of Compound Authorization for Future Research

"However, We Do Not Prescribe Specific Statements in the Rule. We…Agree With Commenters That This Approach Best Harmonizes With Practice Under the Common Rule Regarding Informed Consent for Future Research, and Allows Covered Entities, *Researchers and Institutional Review Boards to Have Flexibility in Determining What Adequately Describes a Future Research Purpose Depending on the Circumstances.*"

Fred Hamilton, JD, Sinai Medical Center of Florida

Compound Authorizations for Future Research – Extrinsic Documents

"[Covered Entities may Use]…a Combined Consent/Authorization Form for a Clinical Trial and Optional Banking Component, With a Check Box for the Individual to Have the Choice to Opt In to the Banking Component, and One Signature, But With the *Detailed Information About the Banking Component Presented in a Separate Brochure or Information* Sheet That is Referenced Directly in the Consent/Authorization Form, [Provided That]…"

Fred Hamilton, JD, Sinai Medical Center of Florida

Compound Authorizations for Future Research – Extrinsic Documents

"…If the Brochure or Information Sheet Includes *Required Elements of the Authorization* (or Informed Consent)…Then the Brochure or Information Sheet Must Be Made Available to Potential Research Participants *Before* They are Asked to Sign the Consent/Authorization Document. …Finally, in Such Cases, a Covered Entity Must Keep Not Only the Signed Consent/Authorization Form, But Also *a Copy of the Brochure or Information Sheet*, in Order to Be in Compliance With the Documentation Requirements at [45 CFR] § 164.530(j)."

Fred Hamilton, JD, Sinai Medical Center of Florida

Practical Tips – "Opt-In" and Opt-Out"

Reviewing the Language, It is Clear That the "Opt-In" Requirement Only Applies if Two Things are True. ***First***, the Research Under Consideration Must Involve Both a "Mandatory" and an "Optional" Component. ***Second***, the Researcher Must Be Seeking Authorization for Uses and Disclosures of Health Information for Both the Mandatory Optional Components in the Same Document (a "Compound Authorization").

Fred Hamilton, JD, Sinai Medical Center of Florida

Example
Compound Authorizations for Future Research

I Hereby Authorize the Use and Disclosure of My Protected Health Information for the Following Purposes:

- ❑ Future Biomedical Research
- ❑ Future Research Into My Disease or Condition
- ❑ Future Research as Described in the Brochure "*Pharmacogenomics and You"* (http://www.pharmacogenomicsandyou.pdf)

Fred Hamilton, JD, Sinai Medical Center of Florida

Questions

- Can a Researcher Review Medical Records to Identify Subjects the Researcher Wants to Recruit? (5 Options)
- If Your Sponsor Requires You to Give Them a Screening Log Can You Send the PHI Outside of the CE? (You May Screen Someone Who May Not Agree to Participate)

Options

1. Authorization
2. IRB/Privacy Board (PB) Waiver
3. Preparatory Work*
4. Decedent Data*
5. Limited Data Set/Data Use Agreement*

*Authorization Not Required

Partial Waiver of HIPAA Authorization

- Authorization May be Temporarily or Partially Waived as a Prelude to Enrollment
  - PHI Sought Solely to Prepare Research Protocol or Identify Potential Subjects
  - PHI May Not be Removed from the Covered Entity
  - Use or Access to the PHI is Necessary for the Research Purpose
  - May or May Not Require HIPAA Authorization to Enroll Subject in Study

45 CFR 164.512

Daniel Nelson and Ina Friedman

Waiver of Authorization

Must Meet the Following Criteria:

1. The Use or Disclosure of PHI Involves No More than Minimal Risk to the Privacy of the Individual
2. The PI Must Provide a Plan to:
   - Protect Identifiers
   - Destroy the Identifiers as Soon as Possible
   - A Statement That the Information Will Not be Disclosed
3. The PI Should Provide Justification as to Why the Research Cannot be Done Without the Waiver.

Joe Brown, University of Kentucky

Waiver of Authorization (Cont'd)

4. The PI Should Provide Justification as to Why the Research Cannot be Done Without the PHI
5. The PI Must Provide a Written Assurance to the IRB/PB that the PHI Will Not be Re-Used or Disclosed Except:
   - As Required by Law,
   - For Authorized Oversight of the Research, or
   - For Other Research that Has Been Reviewed and Approved by the IRB With Specific Approval Regarding Access to this PHI.

Joe Brown, University of Kentucky

Who Has the Authority to Issue a Waiver of Authorization?

- Institutional Review Board (IRB) or a
- Privacy Board (PB)
- Example: Waiver of Authorization Form from University of Kentucky

Questions

- What if a PI is Preparing a New Protocol and to do so Needs to Look at Existing Medical Record Data?
- What if a Researcher Wants to Find Out if There are Enough Potential Subjects to Conduct Research?
- What if PI Wants to Find Out if Usable Data Exists?

Next Option

1. Authorization
2. IRB/Privacy Board (PB) Waiver
3. Preparatory Work*
4. Decedent Data*
5. Limited Data Set/Data Use Agreement*

*Authorization Not Required

Preparatory to Research
Researcher Must Assure:

1. Use Solely to Prepare Protocol
2. No PHI Removed From Covered Entity
3. PHI Necessary for Preparation

Preparatory Research Rule

- Cannot Use Information to Directly Recruit Subjects – Need Partial Waiver of Authorization to Recruit
- If Send Data to Sponsor, Use De-Identified Data or Get a Waiver of Authorization from the IRB or Obtain Authorization – Cannot Use Preparatory if Sending Data Outside of the Covered Entity

Joe Brown, University of Kentucky

To Whom Must the Researcher Submit the Assurance?

- It Depends on the Covered Entity's Policies and Procedures
- May or May Not be Requested in Writing

Case Study

- Dr. Dooright is Director of a Research Specimen Bank/ Repository
- A Mother of a 23 Year Deceased Cancer Patient Wants to Donate Tissue from Her Daughter, Along with Access to Her Daughter's Medical Record.
- What Option Can be Used Under HIPAA?

Next Option

1. Authorization
2. IRB/Privacy Board (PB) Waiver
3. Preparatory Work
4. Decedent Data
5. Limited Data Set/Data Use Agreement

Decedents' PHI
Researcher Must Assure:

1. Use or Disclosure Solely for Research
2. PHI Necessary for Research
3. At Request of Covered Entity, May Need Documentation of Death

To Whom Must the Researcher Provide the Assurance?

It Depends on the Covered Entity

Final Option For Accessing & Sharing

1. Authorization
2. IRB/Privacy Board (PB) Waiver
3. Preparatory Work
4. Decedent Data
5. Limited Data Set/Data Use Agreement

Limited Data Set*

- Limited Types of Identifiers Can Be Released With Health Information
- Can Only Be Released With Data Use Agreement

*No Authorization Required

Limited Data Set Elements

Excluded – Cannot be Released	Included – Can be Released
1. Names (Including Initials)	1. ZIP Codes
2. Street Address*	2. Geocodes
3. Telephone number	3. Dates of Birth
4. Fax Number	4. Other Date Info
5. E-mail Address	5. Any Other Code Not Specified at Left
6. Social Security Number	
7. Medical Record Number	
8. Health Plan Beneficiary #	
9. Account Number	
10. Certificate/License Number	
11. Vehicle Identifiers/Serial #s	
12. Device Identifiers/Serial #s	
13. Web URLs	
14. IP Address Numbers	
15. Biometric Identifiers	
16. Full Face Photographs and Any Comparable Images	

Data Use Agreement Must Include:

- Permitted “Uses”/ ”Disclosures” by the Researcher
- Who is Permitted to Use/Receive the PHI

Data Use Agreement Cont.
Researcher will:

- Not Use/Disclosure Other Than as Permitted
- Use Appropriate Safeguards
- Report to CE Any NOT Permitted Disclosure/Use
- Ensure Subcontractors Agree to SAME Restrictions
- NOT Identify the PHI or Contact Individuals

Limited Data Sets

- If Researcher is Employed in CE…
  - Data Use Agreement Required
- If Outside of the CE…
  - Data Use Agreement Required and a Business Associate Agreement May be Required

HIPAA Extended to Other Entities

- Business Associates
  - Indirect Extension of the Privacy Rule
  - Business Associates are:
    - External Individuals or Entities That Perform a Service on Your Behalf and That Create or Have Access to Identifiable Health Information;
    - Outside Legal, Actuarial, Accounting, Consulting, Management, Administrative, Accreditation, Data Aggregation, and Financial Services That Create or Have Access to Such Information

Business Associates: Written Agreement

- May be Stand-Alone or Part of Larger Contract
- Must Include:
  - Restrictions on How PHI May be Used or Disclosed
  - Promise to Protect the PHI
  - Promise to Return PHI at End of Contract
  - Assurance to Make PHI Available for Compliance

Pearl O'Rourke
Partners Health Care

Business Associates

• Generally NOT a business associate	• Generally Considered a Business Associate
– **Outside Researchers** – **Sponsor** – **Coordinating and Statistical Centers**	- **Web-Hosting/Data-Storage Companies** - **Third Party Billing Company/Consultant** - **Third Party Assisting With Recruitment and/or Screening**

Pearl O'Rourke
Partners Health Care

Who Issues the Data Use Agreements and Business Associate Agreements?

It Depends on Covered Entity Policy and Procedures

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
National Institutes of Health

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

I am a researcher, and my research data source is asking me to sign a business associate agreement. Is this necessary?

Business associates are persons who perform certain services for, or functions or activities on behalf of, the covered entity that require access to PHI, but who are not part of the workforce of the covered entity. If the data source is not a covered entity, no business associate contract is required because the Privacy Rule only applies to covered entities.

If the data source is a covered entity, whether a business associate contract is required depends on the services, functions, or activities that the researcher is providing to or performing for the covered entity. Researchers are not business associates solely by virtue of their own research activities (although they may become business associates in some other capacity, e.g., if de-identifying PHI on behalf of a covered entity). A business associate agreement will typically be a legally enforceable contract, so a researcher may wish to consult legal counsel before signing one.

U.S. Department of Health & Human Services
HHS.gov

Health Services Research and the HIPAA Privacy Rule Commonly Asked Questions and Answers

A covered hospital hired a researcher as a business associate to conduct a quality assessment study using PHI, and the researcher has made some findings that he or she would like to publish for his or her own purposes in a scientific or professional journal. Is this permissible under the Privacy Rule?

U.S. Department of Health & Human Services
HHS.gov

Health Services Research and the HIPAA Privacy Rule Commonly Asked Questions and Answers

Generally not. The business associate agreement between the covered entity and the researcher generally may not authorize the researcher to use or disclose PHI created or received in the researcher's capacity as a business associate for the researcher's own purposes. The business associate agreement also must require that the PHI be returned to the covered entity or destroyed at termination of the contract, if feasible. However,…

U.S. Department of Health & Human Services
HHS.gov

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

a covered entity may provide the researcher with de-identified information that he or she may use for the purposes of preparing the publication or with PHI with individuals' Authorizations for such purpose. In addition, the business associate agreement between the covered entity and the researcher may authorize the researcher to de-identify PHI or to obtain Authorizations from individuals on behalf of the covered entity for publication, even if the researcher is ultimately the intended recipient of the information.

Objective 1: HIPAA Privacy Overview

1. Does HIPAA Apply to Your Research?
2. How Do You Access Data or Share Data Under HIPAA for Research Purposes?
3. What Rights Do the Patient/Subject Have and How Do Those Rights Impact Your Research?
4. Are There Additional Requirements That Impact Research?
5. How Long Must HIPAA Records be Retained?
6. What Penalties Can be Applied if You Do Not Comply With HIPAA Requirements?

What Privacy Rights Has HIPAA Provided Subjects In Research And How Do Those Rights Impact Your Research?

Patient/Subject Privacy Rights

Patients/Subjects Given Rights To:

- Receive Accounting of Disclosures During the Previous 6 Years
- Access Their PHI
- Amend Their PHI
- Revoke Authorization
- Request Restrictions On Uses & Disclosures
- Request Receipt of Communication of PHI By Alternative Means/Locations

How Does the Accounting of Disclosure Right Impact Your Research

- If You are Inside the CE, You May Need to Have a System for Accounting for Disclosures Since Subjects Can Ask for that Accounting
- "Disclosure" is Defined as Sharing Outside the Entity

Researchers Need to Have a System for Accounting of Disclosure Under These Conditions:

- Waiver of Authorization
- Preparatory Research
- Decedent PHI
- Disclosure to Public Health Authorities
- Disclosure Mandated By Law

Researchers Not Required to Have a System for Accounting of Disclosure Under These Conditions:

- Authorization
- Limited Data Sets With Data Use Agreement
- Disclosure Made to the Patient/Subject
- De-identified Information

Right to Accounting of Disclosures

For Each Disclosure, Must Record:

- List of Individuals
- Date of Disclosure
- Name of Person/Entity Who Received it All (and Their Address, if Known)
- Brief Description of PHI Disclosed
- Brief Statement of the Purpose of the Disclosure

Johns Hopkins Form Attached

Pearl O'Rourke
Partners Health Care

Right to Accounting of Disclosures

- Modified Tracking Mechanism Available for Research Involving the Disclosure of PHI from 50 or More Subjects
  - Entity Does Not Have to Maintain List of Specific Individuals

Pearl O'Rourke
Partners Health Care

Modified Tracking Mechanism (Cont'd)

- Entity Must Provide Upon Request:
  - Name and Description of All Protocols Involving Disclosure of 50 or More Subjects
  - Brief Description of the Types of PHI Disclosed
  - Dates or Time Periods of the Disclosures
  - Contact Information of the Recipients
  - Statement that a Specific Individual's PHI May or May Not Have Been Disclosed for a Particular Study
- Entity Must Assist the Individual, if Requested, in Contacting the Likely Recipients of PHI

Bottom Line

- If You are In the CE, Advise That You Contact Your Privacy Officer for Advice on How Your CE Wants You to Account for Disclosures
- If You are Not In the CE…

What Other Patient Rights Might Impact Your Research?

Patient/Subjects Can Ask for Access to Their PHI

Right to Access Their PHI

- Access = Inspect and Copy
- Limited to PHI Maintained in a "Designated Record Set"
  - Medical and Billing Records and Any Records Used to Make Decisions About Individuals
  - Includes PHI Generated in Research and:
    - Recorded in Medical Charts or Billing Records
    - Recorded Elsewhere and Used to Make Clinical or Billing Decisions About the Subject

Pearl O'Rourke
Partners Health Care

Right to Access Their PHI

- Right to Access Can be Temporarily Suspended While the Research is in Progress, if Stated in the Signed Authorization
- There are Limited Other Exceptions to Access

Pearl O'Rourke
Partners Health Care

What is Another Patient Right That Might Impact Your Research?

Patient/Subjects Have a Right to Amend Their PHI

Right to Request Amendment

- Limited to PHI Maintained in a "Designated Record Set"
- Entity Must Have a Process for Determining Whether or Not Request is Appropriate
- If Request is Granted, Researcher Will Work With the Privacy Officer to Accommodate/Implement the Request

Pearl O'Rourke
Partners Health Care

Another Patient Right is…

Right to Revoke Authorization

- Revocation Must be in Writing
- If Research Authorization is Revoked, Researcher Cannot Use or Disclose the PHI, Except to the Extent that the Researcher has Already Relied on the Permission:
  - If the Researcher has Already Included the PHI in an Analysis
  - If Use or Disclosure is Needed to "Maintain the Integrity of the Research Study (i.e., Account for Withdrawal, Report Adverse Event)

Pearl O'Rourke
Partners Health Care

Another Patient Right is…

Right to Request Alternate Means/ Location of Communication of PHI

- E.g., Home Address vs. Work Address
- Entity Must Accommodate Reasonable Requests
- Entity May Not Require the Individual to Explain the Basis for the Request

Go to Your Privacy Officer for Advice

Pearl O'Rourke
Partners Health Care

Another Patient Right is…

Right to Request Restrictions

- Individuals Can Request Restrictions on Uses and/or Disclosures of Their PHI
- Entity Can Determine Whether Request is Appropriate and Feasible
- If Request is Granted, the Restriction Must be Followed, and Researcher Should Work With the Privacy Officer to Accommodate/Implement the Restriction

Pearl O'Rourke
Partners Health Care

What Additional HIPAA Requirements Impact Research?

Additional Requirements

- Mandatory Education (Check with the Covered Entity)
- Psychotherapy Notes
- Minimum Necessary Standards

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

What special requirements apply to research involving PHI from mental health providers?

The Privacy Rule provides individuals special protection for psychotherapy notes, which are notes recorded by a mental health provider that document or analyze counseling session conversations, and are maintained separately from the medical record. Unless the covered provider obtained, prior to the compliance date, the individual's informed consent or other express legal permission for the research or an IRB waiver of informed consent for the research, a covered entity may not use or disclose these notes for research without the individual's written Authorization.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

What special requirements apply to research involving PHI from mental health providers? (Continued)

Information in the medical record and certain types of information, even if maintained separately from the medical record (e.g., information about test results, length and frequency of treatment, diagnosis, symptoms, or progress), is excluded from the definition of psychotherapy notes and may be released to researchers who obtain an Authorization or a waiver of Authorization from an IRB or Privacy Board, as part of a limited data set, or if appropriate, for reviews preparatory to research or for research involving decedent's information where required representations are obtained. Special requirements also apply to compound authorizations involving the use or disclosure of psychotherapy notes. (See section 164.508(b)(3)(ii) of the Privacy Rule.) Various state laws governing the use or disclosure of mental health records, including psychotherapy notes, which are more stringent than the Privacy Rule provisions, may also apply.

"Minimum Necessary" Standard Applies in Research

A Covered Entity Must Try to Limit the PHI it Uses, Discloses, or Requests to the "Minimum Necessary" to Achieve the Purposes

"Minimum Necessary" Standard Applies to the Following 4 Options:

- Waiver of Authorization
- Use/Disclosures of Decedent's PHI
- Uses Preparatory to Research
- Limited Data Sets

Pearl O'Rourke
Partners Health Care

"Minimum Necessary" Standard DOES NOT APPLY:

- Use or Disclosure Made With an Authorization
- Treatment Disclosures or Requests
- Disclosures to/Uses by the Subject at the Subject's Request
- Disclosures to DHHS for Compliance; Other Uses and Disclosures for Compliance
- Uses or Disclosures as Required by Law

Pearl O'Rourke
Partners Health Care

How Long Must HIPAA Documentation Be Retained?

Documentation (See Rule for Additional Requirements)

Document	Retained by	Length of retention
Authorization Form	**Covered Entity**	**6 Years from Date of Creation or from Date When Last in Effect, Whichever is Later**
Data Use Agreement		
Written Revocation		
Waiver of Authorization		
Access to Designated Record Set		
Accounting for Disclosures Made After the Compliance Date		

What Penalties Apply if HIPAA Non-Compliant?

Penalties

Civil Fines:
$100 Per Violation (Min): $50K Per Violation (Max) … Up to 1.5 Million (Annual Maximum)

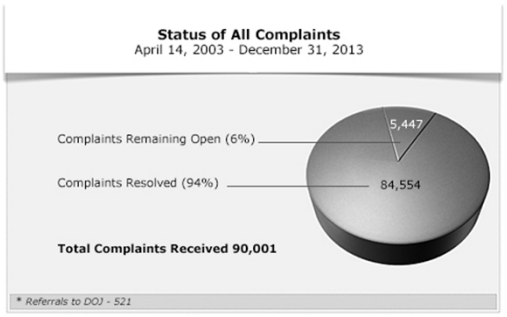
Criminal Penalties:
Significant Fines and Imprisonment (Up to 1 Year for Knowing Violations; Up to 10 Years for Violations With Intent of Personal Gain or Malicious Harm)

Overseen by the Office of Civil Rights & the Department of Justice

Select HIPAA Violations

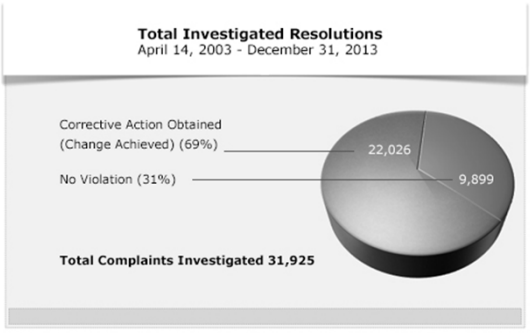
- 12/26/13: Unencrypted Flash Drive = $150,000
- 9/17/12: Theft of Unencrypted Laptop, PHI of Patients and Research Subjects = $1,500,000
- 4/18/12: Publicly Accessible Internet Appointment Calendar = $100,000
- 2/24/11: PHI Documents Left on Subway = $1,000,000
- 2/22/11: Denied Patient Access to Their Medical Records Plus Refusal to Respond to OCR's Demands = $4,300,000

U.S. Department of Health & Human Services
HHS.gov



http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/indexnumbers.html

U.S. Department of Health & Human Services
HHS.gov



http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/indexnumbers.html

amednews.com http://www.amednews.com/article/20100607/business/306079969/6/

HIPAA violation leads to jail time
The case, involving a former UCLA employee, is the first to result in incarceration for unauthorized access of patient medical records.
By Pamela Lewis Dolan— Posted June 7, 2010

Huping Zhou, a licensed cardiothoracic surgeon in China who was working at the UCLA School of Medicine as a researcher in 2003, was sentenced in late April to four months in jail after pleading guilty to charges related to looking at patient medical records he was not authorized to view.

According to experts, Zhou's incarceration, the first in the nation for looking at patient files without a valid reason, should serve as a warning sign to all medical practices that times have changed when it comes to patient privacy.

"There's no question that this is sending a message," said Stephen Aborn, executive director of Andrews International, a Valencia, Calif.-based investigative and security services provider. That message: Health care organizations, and their employees, can't afford to be complacent about privacy of patients' electronic data.

U.S. Department of Health & Human Services
HHS.gov

May 10, 2013

Idaho State University Settles HIPAA Security Case for $400,000

Idaho State University (ISU) has agreed to pay $400,000 to the U.S. Department of Health Human Services (HHS) for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This settlement involves the breach of unsecured electronic protected health information (ePHI) of 17,500 individuals who were patients at an ISU clinic.

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement.html

Objective 1: HIPAA Privacy Overview

1. Does HIPAA Apply to Your Research?
2. How Do You Access Data or Share Data Under HIPAA for Research Purposes?
3. What Rights Do the Patient/Subject Have and How Do Those Rights Impact Your Research?
4. Are There Additional Requirements That Impact Research?
5. How Long Must HIPAA Records be Retained?
6. What Penalties Can be Applied if You Do Not Comply With HIPAA Requirements?

Objective 2

- Identify Differences Between HIPAA and IRB Regulations

IRB vs. HIPAA
Differences/Implications

- Penalties
- Applicability
- Exemption vs. De-Identification
- Consent vs. Authorization
- IRB/Waiver of Consent vs. HIPAA Waiver of Authorization
- Preparatory Work
- Decedent Data

IRB vs. HIPAA
Differences/Implications (Continued)

- Limited Data Set/Data Use Agreements
- Minimum Use Standard
- Accounting of Disclosures

Penalties

IRB	HIPAA
• No Civil/Criminal Penalties (State Law)	• Fines Up to 1.3 Million
• Regulatory Disqualification/ Eligibility to Conduct Research or Receive Funds [Individual or for Institution]	• Imprisonment

Applicability: Definition of "Human Subject"*

A Living Individual About Whom an Investigator… Conducting Research Obtains (1) Data Through Intervention or Interaction with the Individual, or (2) Identifiable Private Information

*45 CFR 46.102(f)

HIPAA

- Includes Deceased Individuals

Implication?

Study/Research Activity that Does Not Fall Under IRB May Fall Under HIPAA

Exemption vs. De-Identification

"Research involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects."

IRB Exemption
"Cannot Be Identified"

- Direct Identifiers: Not Defined in the IRB Regulations
- No Indirect Link: Code List

HIPAA
"Cannot Be Identified" is Defined

- If Any of 18 Identifiers Included – HIPAA Applies

De-Identification Involves Removing These Identifiers:

- Names (individual, employer, relatives, etc.)
- Address (street, city, county, zip code - more than 3 digits, or any other geographical codes)
- Telephone/Fax Numbers
- Social Security Numbers
- Dates (except for years)
  - Birth Date
  - Admission Date
  - Discharge Date
  - Date Of Death
- All ages > 89 and all elements of dates indicative of such age (except that such age and elements may be aggregated into a category "Age > 90"
- E-mail addresses/URLs
- Medical Record Numbers
- Health Plan Beneficiary Numbers
- Account Numbers
- Certificate/License Numbers
- Vehicle Identifiers and Serial Numbers (e.g. VINs, License Plate Numbers)
- Device Identifiers and Serial Numbers
- Biometric Identifiers (e.g. finger or voice prints) or Photographs
- Any other unique identifying number, characteristic, or code

Exemption vs. De-Identification Implications

- Studies Exempt From IRB May Fall Under HIPAA

IRB Access vs. HIPAA Access

IRB	HIPAA
• Informed Consent	• Authorization
• Waiver of Consent	• Waiver by IRB/PB*
• Waiver of Documentation	• Not Discussed
• Not Discussed	• Preparatory Work
• Living Individual	• Decedent Data
• Not Discussed	• Limited Data Set/Data Use Agreement

*Only HIPAA Requirement That Uses IRB/Privacy Board

Informed Consent vs. Authorization

IRB	HIPAA
• 8 Elements	• 6 Core Elements
• 6 Additional Elements	• 3 Required Statements
• General Conditions	• 2 Additional Requirements
• Focus on Protocol	• Focus on PHI

Authorization
2 Additional Requirements

IRB	HIPAA
• Understandable Language	• Plain Language
• Copy of Consent Document	• Copy of Signed Authorization

164.508(c)(3) & (4)

IRB/PB Waiver

IRB	HIPAA
• 4 Criteria	• 3 Criteria With 3 Sub-Requirements
• Focus Entire Protocol	• Focus PHI
• Approval Letter Study	• Signature Chair PB/IRB Identified

IRB/PB Waiver of Authorization

IRB	HIPAA
1. "Minimal Risk" Study	1. "Minimal Risk" to Privacy Based On 3 Elements: Plan to Protect; Plan to Destroy Identifiers; Written Assurance Will Not be Reused or Disclosed
2. Rights & Welfare Not Adversely Affected	2. Not Discussed

IRB/PB Waiver of Authorization

IRB	HIPAA
3. Research Could Not Practicably be Conducted Without Waiver	3. Same as IRB
4. Not Addressed	4. Research Could Not Practicably be Conducted Without Access to & Use of PHI

Waiver Implications

- Apply 2 Different Sets of Criteria
- Can Result in Different Conclusions

Access to PHI Without Authorization

IRB	HIPAA*
• Not Discussed	• Preparatory Work
• Living Human Subjects	• Decedent Data
• Not Discussed	• Limited Data Set/Data Use Agreement

*No Requirement that Review Must be Conducted by IRB or a Privacy Board

Additional HIPAA vs. IRB Differences

IRB	HIPAA
• Not Discussed	• Minimum Use Standard
• Not Discussed	• Accounting of Disclosures
• Unanticipated Problems, Serious or Continuing Noncompliance, Suspension or Termination	• Notification of Breaches

Objective 3

- To Share a Select List of Frequently Asked Questions

See Handout

JOHNS HOPKINS MEDICINE

1

HIPAA Questions & Answers Relating to Research: The Basics

How is the HIPAA Privacy Rule related to the HIPAA Security Rule?

Each is a separate regulation under the HIPAA statute. The Privacy Rule applies to all health information obtained or created by a covered entity, regardless of medium. The Security Rule applies to protected health information created or stored in an electronic form. The Security Rule establishes standards for how covered entities store, transmit, and safeguard electronic PHI.

JOHNS HOPKINS MEDICINE

2

HIPAA Questions & Answers Relating to Research: The Basics

I am a researcher who has obtained a Certificate of Confidentiality for my study. Do I need a HIPAA Privacy Authorization when I already have a Certificate of Confidentiality?

Yes. Certificates of Confidentiality (CoCs) may protect the identities of research participants from compulsory disclosure in certain legal proceedings. However, COCs do not prevent voluntary disclosures of research information, nor do they negate the fact that researchers collect PHI from participants and that many persons both inside and outside of the covered entity will or may see the PHI (e.g., auditors, IRBs, investigators from governmental agencies, sponsors, etc.) Accordingly, the HIPAA Privacy Authorization must inform participants that, although researchers will keep their identifiable information confidential, there are certain people in and outside of the covered entity who will or may need to see the information, and that, because some of those people are not covered by the Privacy Rule, we cannot guarantee that they will all maintain the confidentiality of the information.

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

A researcher requests data that assigns a code derived from the last four digits of the social security number. This code is necessary to link individual records from different data sources. The data contain none of the other listed HIPAA identifiers at section 164.514(b)(2). Are the data de-identified under the Privacy Rule?

No. Under the Privacy Rule, a de-identified data set may not contain unique identifying codes, except for codes that have not been derived from or do not relate to information about the individual and that cannot be translated so as to identify the individual. A code derived from part of a social security number, medical record number, or other identifier does not meet this test.

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

Are an individual's initials considered to be identifiers under the Privacy Rule?

Yes, because an individual's name is an identifier and initials are derived from the individual's name, initials are considered identifiers under the Privacy Rule. Thus, for information to be de-identified using the safe harbor method of the Privacy Rule, an individual's initials must be stripped from the information. However, it may be possible for initials to remain as part of de-identified information if the statistical method for de-identification at section 164.514(b)(1) allows it.

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

How does the Privacy Rule apply to research involving blood or tissue samples?

Under the Privacy Rule, neither blood nor tissue, in and of itself, is considered individually identifiable health information; therefore, research involving only the collection of blood or tissue would not be subject to the Privacy Rule's requirements. Remember, however, blood and tissue are often labeled with information (e.g., admission date or medical record number) that the Privacy Rule considers individually identifiable and thus, PHI. A covered entity's use or disclosure of this information for research is subject to the Privacy Rule. In addition, the results from an analysis of blood and tissue, if containing or associated with individually identifiable information, would be PHI.

U.S. Department of Health & Human Services
HHS.gov

6

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

I am a health services researcher employed by a university that has designated itself as a "hybrid entity" for purposes of the Privacy Rule. The university's hospital and medical school are within the "health care component" of the hybrid entity, but my epidemiology department is not. Am I subject to the Privacy Rule requirements that apply to the health care component of the university?

U.S. Department of Health & Human Services
HHS.gov

6

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

No. The Privacy Rule permits a covered entity that performs both covered and noncovered functions as part of its business operations to elect to be a hybrid entity. A covered function is any function, the performance of which makes the entity a health plan, health care provider, or health care clearinghouse. To become a hybrid entity, the covered entity must designate and include in its health care component(s) all components that would meet the definition of a covered entity if that component were a separate legal entity. In addition, a covered entity may include in its health care component any component that functions as a noncovered health care provider or that performs activities that would make the component a business associate of the entity if it were legally separate.

However, the hybrid entity is not permitted to include in its health care component other types of components that do not perform the covered functions of the covered entity. For example, a university that has designated its hospital and medical school as the health care component may not also include a component that performs records research that is not used to support the covered functions of the health care component.

U.S. Department of Health & Human Services
HHS.gov

6

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

Within the hybrid entity, most of the Privacy Rule requirements apply only to the health care component(s), although the hybrid entity retains certain oversight, compliance, and enforcement obligations. See section 164.105 of the Privacy Rule for more information.

Remember, however, that a health care component must comply with the Privacy Rule when using or disclosing PHI, including when sharing PHI with a non-health care component of a hybrid entity. Thus, for a health care component of a covered entity to disclose PHI to a researcher in a non-health care component of the entity, the disclosure of PHI must be permitted either by the individual's Authorization or by one of the Privacy Rule's exceptions to the Authorization requirement, such as a waiver of Authorization granted by an IRB or Privacy Board. In addition, since the Privacy Rule treats the sharing of PHI from the health care component to any non-health care component as a disclosure, a health care component's sharing of PHI with another component of the hybrid entity for research purposes may, in certain cases, be subject to the Privacy Rule's accounting requirements. See section 164.528 of the Privacy Rule.

I am conducting a large research study in which I will obtain data from multiple covered entities. Must each covered entity disclosing data to me for my research receive documentation that its own IRB or Privacy Board has granted my project a waiver of Authorization?

No. The Privacy Rule permits covered entities reasonably to rely upon a researcher's documentation that a waiver was properly granted by a single IRB or Privacy Board, even if the IRB or Privacy Board is not affiliated with the covered entity. Under the Privacy Rule, one IRB or Privacy Board's documentation of waiver of Authorization suffices.

May a covered entity that performs research create de-identified health information to be used to prepare a grant application for research as part of its health care operations, or is this activity a review preparatory to research?

Creating de-identified health information from PHI is a health care operation. Thus, to de-identify PHI, a covered entity that performs research need not have representations as required for a review preparatory to research, and the covered entity's subsequent use or disclosure of the de-identified information is not subject to the Privacy Rule. A covered entity is also permitted to hire a business associate to de-identify PHI.

Is a covered entity's patient list that includes only names and addresses considered to be PHI if there is no other health or payment information attached?

Yes, because the names are in a context that indicates that the individuals named were patients of the covered entity. See the Privacy Rule's definition of "individually identifiable health information" at section 160.103, which explicitly includes demographic information collected from an individual.

U.S. Department of Health & Human Services
HHS.gov

10

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

May a covered entity rely on an Authorization signed by parent on behalf of a minor child, even after the child has reached the age of majority? Similarly, would the Privacy Rule's transition provisions "grandfather" an informed consent signed by a minor's parent even if the child reached the age of majority before the Privacy Rule compliance date?

Yes. A valid Authorization signed by a parent, as the personal representative of a minor child at the time the Authorization is signed, remains valid until it expires or is revoked, even if such time extends beyond the child's age of majority. If the Authorization expires on the date the minor reaches the age of majority, the covered entity would be required to obtain a new Authorization form signed by the individual in order to further use or disclose PHI covered by the expired Authorization.
In addition, the Privacy Rule's transition provisions at section 164.532(c) "grandfather" permissions for research (e.g., an informed consent) obtained prior to compliance with the Privacy Rule (usually, April 14, 2003).
Therefore, even if the child has reached the age of majority, the Privacy Rule "grandfathers" a parent's consent on behalf of his or her minor child for research so that the consent remains valid until it expires or is withdrawn.

U.S. Department of Health & Human Services
HHS.gov

11

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

Does the Privacy Rule permit a researcher who is a covered workforce member of a covered entity to transfer PHI, without individual Authorization, to another institution if, for example, the researcher changes jobs?

No, unless the original permission under which the researcher obtained or created the data (such as the individual's Authorization or a waiver by an IRB) was granted explicitly for the researcher himself or herself, rather than solely for the covered entity. Otherwise, any transfer of PHI from one covered entity to another entity for these research purposes must be done according to a new permission (Authorization, waiver, etc.) that covers such disclosure.

JOHNS HOPKINS MEDICINE

12

HIPAA Questions & Answers Relating to Research: The Basics

When might I need a HIPAA Data Use Agreement in connection with my research?

A Data Use Agreement is needed when a researcher wants to share PHI in the form of a Limited Data Set with someone not otherwise involved in the research protocol (i.e., someone who is not mentioned as receiving PHI in the Authorization or in the waiver of Authorization approved by the IRB). If the person or entity at the other site is part of the trial and is included in the Authorization or waiver of Authorization approval for the trial, you do not need a Data Use Agreement. Rather, a Data Use Agreement is used when, for example, you want to share a Limited Data Set of research data with a colleague at another institution not involved in the trial, or with a private registry not involved in the study.

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

What is a limited data set, and what are its advantages?

A limited data set is PHI that does not include a specified list of direct identifiers. The limited data set is not considered to be de-identified information, and unlike de-identified information, a limited data set may include identifiers such as ZIP codes, elements of dates, and unique identifiers not listed as direct identifiers at section 164.514(e). The advantage of a limited data set is that even though it is not de-identified, it can still be used or disclosed for research purposes without an Authorization or a waiver of the Authorization requirement. A covered entity must, however, enter into a data use agreement with the recipient of the limited data set before using or disclosing it. (See section 164.514(e) of the Privacy Rule.)

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

What types of information (direct identifiers) must be omitted from PHI in order to qualify the information as a limited data set?

All the following direct identifiers of the individual or of relatives, employers, or household members of the individual must be removed:

- Name
- Street name or street address or post office box (i.e., not including city, state, or ZIP code)
- Telephone and fax numbers
- Email address
- Social security number
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- URLs and IP addresses
- Full-face photos and other comparable images
- Medical record numbers, health plan beneficiary numbers, and other account numbers
- Device identifiers and serial numbers
- Biometric identifiers, including finger and voice prints

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

May a limited data set include the geographic subdivision code with the five-digit ZIP code (or a nine-digit ZIP code)?

Yes, the limited data set may include the five-digit or nine-digit ZIP code plus any other geographic subdivision, such as state, county, city, precinct, and their equivalent geocodes, except for street name or street address or post office box.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

16

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

What is the difference between a de-identified data set and a limited data set?

A de-identified data set is one in which either: (1) The 18 identifiers specified in 164.514(b)(2)(i) have been removed and the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify the individual (safe harbor method); or (2) a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, determines the risk is very small that the information could be used by the recipient, alone or in combination with other reasonably available information, to identify an individual (section 164.514(b)(1)), and documents the basis for such determination. A de-identified data set is not protected by the Privacy Rule and may be used and disclosed without restriction.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

16

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

A limited data set is one that excludes the direct identifiers in 164.514(e)(2). Unlike a de-identified data set, a limited data set is PHI because it may include dates, city, state, and ZIP codes, and other unique identifying codes or characteristics not listed as direct identifiers. A limited data set may be used or disclosed, without Authorization, for research, public health, or health care operations purposes, in accordance with section 164.512(e), only if the covered entity and limited data set recipient enter into a data use agreement. However, if the use or disclosure could be made under another provision of the Privacy Rule, such as for public health purposes in accordance with section 164.512(b), such agreement is not required.

U.S. Department of Health & Human Services HHS.gov

17

Health Services Research and the HIPAA Privacy Rule Commonly Asked Questions and Answers

May a limited data set include a unique code or identifier not listed at section 164.514(e)(2) of the Privacy Rule?

A limited data set may include unique codes or identifiers not listed as direct identifiers at section 164.514(e)(2) of the Privacy Rule, provided the code or identifier does not replicate part of a listed direct identifier. For example, a limited data set may not include the last four digits of a Social Security number or an individual's initials since these identifiers are elements of, or replicate part of, a direct identifier. However, the limited data set may include a code that is derived from the individual's direct identifier as long as it does not replicate any part of the direct identifier. In any event, before a covered entity may use or disclose a limited data set, the recipient of the information must be restricted by a data use agreement from re-identifying the information or contacting the subjects of the information. See section 164.514(e)(4)(ii) for additional content requirements of the data use agreement.

U.S. Department of Health & Human Services
HHS.gov

18

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

I work for a covered entity and conduct observational studies on patients' reactions to various emergency room triaging. The nature of the study requires that individuals not know they are being observed. Under HHS Protection of Human Subjects Regulations, the IRB is allowed to waive the informed consent requirement when certain criteria are met. Must I also receive documentation of an IRB waiver of the Authorization requirement under the Privacy Rule for observational studies?

U.S. Department of Health & Human Services
HHS.gov

18

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

It depends on whether the study is research, as defined by the Privacy Rule. The Privacy Rule distinguishes between research and studies for quality assessment and improvement purposes based on whether the *primary* purpose of the study in question is to obtain generalizable knowledge. The Privacy Rule defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

U.S. Department of Health & Human Services
HHS.gov

18

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

If the primary purpose of such a study is to obtain generalizable knowledge, then the activity does not meet the definition of a "health care operation" and, instead, meets the definition of "research," and any use or disclosure of PHI for such study must be made in accordance with the Privacy Rule's provisions for the use and disclosure of PHI for research. For example, an IRB or a Privacy Board may waive or alter the Authorization requirement, as long as certain criteria at…

section 164.512(i)(2)(ii) are met (i.e., the use or disclosure of PHI involves no more than minimal risk to the privacy of individuals and the research could not practicably be conducted without the requested waiver or alteration or without access to and use of the PHI).

If, however, a covered entity is conducting a quality improvement or assessment study, the primary purpose of which is not to develop or contribute to generalizable knowledge, then…

the study is considered to be a health care operation, and the covered entity may use or disclose PHI for the study as part of its health care operations under the Privacy Rule. The Privacy Rule does not require documentation of an IRB or Privacy Board waiver or alteration of Authorization for uses and disclosures of PHI for health care operations activities. Nor does the Privacy Rule require the individual's Authorization for uses and disclosures of PHI for health care operations activities.

Does a covered entity need to account for disclosures of PHI contained in a limited data set?

No. The accounting requirement does not apply to limited data set disclosures.

JOHNS HOPKINS MEDICINE

20

HIPAA Questions & Answers Relating to Research: Recruitment

At what point in recruitment may we gather information about a potential participant (i.e., a potential participant calls our office after seeing a flier, may we screen that person/ ask them about their history, or do we need him or her to complete a written privacy Authorization prior to screening)?

If the IRB has approved your recruitment plan, including a partial waiver of Authorization to permit you to collect PHI for screening without written Authorization, you may take the person's contact and screening information. You will need to advise the person that in order to evaluate whether he or she is a candidate for the research, you will need to share the caller's information, and the caller may need to share information, with a limited number of others who staff the study. If the person is deemed to be a qualified candidate, then he/she will be asked to come in to sign an informed consent/privacy Authorization.

If the person is not deemed to be qualified, their information should be destroyed and not used for any other purpose, unless the IRB has waived authorization to permit the research team to retain information required by the sponsor or by FDA regulations.

JOHNS HOPKINS MEDICINE

21

HIPAA Questions & Answers Relating to Research: Recruitment

When a potential participant calls after seeing a flier, may we take a history from the participant to determine eligibility prior to receiving a written privacy Authorization if we do not record (either in a database or written form) the PHI given to us by the participant?

The answer is the same as in #1, above. Receipt of PHI occurs whether the information is written, electronic or verbal. The IRB must approve the recruitment plan to permit phone screening for eligibility. The PI or research team must receive the follow-up written Authorization before they may use the PHI for research.

JOHNS HOPKINS MEDICINE

22

HIPAA Questions & Answers Relating to Research: Recruitment

When the potential participant calls our office, may the staff member who took the call have another staff member (same research team) send materials to/contact the potential participant?

Yes. Anyone on the research team or staff may use the contact information to send materials to prospective subjects and to obtain the Authorization.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

May a covered health care provider discuss with a patient his or her enrollment in clinical research without the patient's Authorization? What if the individual is not a patient of the covered provider?

Yes. These types of conversations may arise under a variety of circumstances. For example, a physician may for treatment purposes discuss treatment alternatives with the individual, which may include the option of enrolling in a clinical trial. In addition, a physician may speak to the individual about a clinical trial as part of asking the individual to sign an Authorization to permit the covered provider to use or disclose the individual's PHI for the research study. Also, the Privacy Rule generally permits a covered entity to communicate with individuals and to disclose their PHI to them. Therefore, covered health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient Authorization, regardless of whether the individual is a patient of the covered provider, and without an IRB or Privacy Board waiver of the Authorization. However, the covered health care provider must obtain the individual's Authorization or an IRB or Privacy Board waiver of Authorization, or meet certain other conditions, before using or disclosing the individual's PHI as part of the research study.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

Similarly, if a physician knows of a study in which his or her patient might enroll that is being conducted by others, the physician may discuss such a trial with the patient and give the patient the researcher's contact information so the patient may contact the researcher directly. However, the physician may only contact the researchers about the patient so long as de-identified information is disclosed, the individual's Authorization or IRB or Privacy Board waiver of Authorization is obtained, or other conditions that satisfy the Privacy Rule are met. For example, it is acceptable to give a clinical summary of a patient to a researcher to determine if the patient might meet enrollment criteria, if such discussions omit the patient's name, address, medical record number, and any other identifying information set forth in section 164.514(a)-(c) of the Privacy Rule.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

May a covered entity obtain an individual's Authorization to include his or her PHI in a clinical research recruitment database of possible research participants, such as a pre-screening log?

Yes. The Privacy Rule permits a covered entity to include an individual's PHI in a clinical research recruitment database and permit researchers access to the recruitment database, provided the individual has given permission through a written Authorization. The Authorization must inform the individual of the purpose for which (e.g., for the pre-screening log for one or more clinical trials) and what PHI will be used and meet the other requirements at section 164.508 of the Privacy Rule. Alternatively, a covered entity may provide a researcher access to the PHI for reviews preparatory to research, provided the required representations are obtained. See section 164.512(i) of the Privacy Rule. Unless otherwise permitted by the Privacy Rule, a subsequent Authorization must be obtained from the individual before a covered entity may use or disclose the individual's PHI for the clinical trial itself.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

25

Clinical Research and the HIPAA Privacy Rule: Frequently Asked Questions and Answers

One common method for recruiting research participants involves organizing a call center for potential research participants to contact in response to advertisements about the research. Would a call center be required to obtain the individual's Authorization before speaking to the individual about the trial?

Call centers in many cases will not be part of a covered entity (health plan, health care clearinghouse, certain health care providers), and thus, are not required to comply with the Privacy Rule. A call center for research is an entity established to receive and answer calls from interested individuals about a research project. Commonly, a call center will collect identifiable information about a caller who may be interested in the research study and then transmit such information to researchers involved in the study or send information about a study directly to callers.

If a call center is part of a covered entity, e.g., part of a covered health care provider that is also a researcher, it may speak with an individual without Authorization for purposes of communicating about the research study or obtaining the individual's Authorization to use or disclose his or her PHI for the study. However, any use or disclosure of the individual's PHI for the research study itself or other purposes is subject to the conditions set forth in the Privacy Rule.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

26

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

May a covered entity use or disclose PHI to locate or identify the whereabouts of a research participant (e.g., subjects who are "lost to follow-up")?

A covered entity is permitted to use or disclose PHI to identify or locate the whereabouts of a research participant during the study as long as the use or disclosure is not limited in the individual's Authorization (or grandfathered prior permission, if relevant) or waiver or alteration of Authorization. In addition, such use or disclosure is permissible if, for example, it is necessary for treatment of the individual or for a permissible public health purpose.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

27

NIH Research Repositories, Databases, and the HIPAA Privacy Rule Frequently Asked Questions & Answers

I am a researcher, and my research data source is asking me to sign a business associate agreement. Is this necessary?

Business associates are persons who perform certain services for, or functions or activities on behalf of, the covered entity that require access to PHI, but who are not part of the workforce of the covered entity. If the data source is not a covered entity, no business associate contract is required because the Privacy Rule only applies to covered entities.

If the data source is a covered entity, whether a business associate contract is required depends on the services, functions, or activities that the researcher is providing to or performing for the covered entity. Researchers are not business associates solely by virtue of their own research activities (although they may become business associates in some other capacity, e.g., if de-identifying PHI on behalf of a covered entity). A business associate agreement will typically be a legally enforceable contract, so a researcher may wish to consult legal counsel before signing one.

JOHNS HOPKINS MEDICINE

28

HIPAA Questions & Answers Relating to Research: Subject Requests for Access to Research Data or Test Results

Do the HIPAA requirements allow for participants to request a copy of any structured interviews they completed/responded to as part of the study? What about the results of research laboratory tests?

Individuals have a right to a copy of their "designated record set".

JOHNS HOPKINS MEDICINE

29

HIPAA Questions & Answers Relating to Research: Subject Requests for Access to Research Data or Test Results

I am enrolling subjects in a clinical study. If adverse events occur and my subjects are treated by another provider, how may I obtain information about the subjects' treatment?

A subject must sign an Authorization that allows the another provider to disclose PHI to you for the purposes of research involving that subject. It is helpful to obtain the subject's express permission for such a disclosure in the Authorization form that the subject signs for your research study. The other provider may rely upon such Authorization; alternatively, the provider may ask the patient to sign the provider's own Authorization, or may disclose the records directly to the patient.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES National Institutes of Health

30

Clinical Research and the HIPAA Privacy Rule: Frequently Asked Questions and Answers

If, under the "preparatory to research" provisions, a researcher identifies subjects that meet the study's eligibility criteria, how can the researcher contact the potential participant to obtain Authorization after identifying these individuals?

Under the "preparatory to research" provision, covered entities may use and disclose to researchers PHI to aid in study recruitment. They may allow a researcher to identify, but not contact, potential study participants. In order to contact potential study participants, a researcher may do so, without Authorization from the individual, under the following circumstances:

- If the researcher is a workforce member of a covered entity, the researcher may contact the potential study participant, as part of the covered entity's health care operations, for the purposes of seeking Authorization. Alternatively, the covered entity may contract with a researcher as a business associate to assist in contacting individuals on behalf of the covered entity to obtain their Authorizations.
- If the covered entity obtains documentation that an IRB has partially waived the Authorization requirement to disclose PHI to a researcher for recruitment purposes, the covered entity could disclose to the researcher that PHI necessary for the researcher to contact the individual.

U.S. Department of Health & Human Services
HHS.gov

31

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

May a covered entity hire a researcher as a business associate to de-identify health information when the researcher is the intended recipient of the de-identified data?

Yes. A covered entity may hire the intended recipient of the de-identified data as a business associate for purposes of creating the de-identified data. That is, a covered entity may provide a business associate that is also the de-identified data recipient with PHI, including identifiers, so that the business associate can de-identify the data for the covered entity.

However, the data recipient, as a business associate, must agree in its business associate agreement to return or destroy the identifiers once the de-identified data set has been created.

U.S. Department of Health & Human Services
HHS.gov

32

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

May a covered entity that has hired a researcher as its business associate for the purposes of de-identifying data permit the researcher to assign to the de-identified data a re-identification code, if the researcher is also the intended recipient of the de-identified data?

Yes, provided the researcher is able to return or destroy all identifiers once the de-identified data set has been created, as required by her or his business associate contract. This would include the researcher's providing to the covered entity the mechanism for re-identification (the code key) and retaining no copy or other method of re-identification. In cases where the researcher has a standard method for assigning a re-identification code that necessarily remains with the researcher even after the other identifiers have been returned or destroyed, the information is not considered de-identified if the researcher assigns such a re-identification code.

U.S. Department of Health & Human Services
HHS.gov

33

Health Services Research and the HIPAA Privacy Rule
Commonly Asked Questions and Answers

Is a covered entity permitted, as part of its health care operations activities, to disclose PHI to a business associate to create de-identified data or a limited data set that may function as a research database? Or does the covered entity need an Authorization or a waiver or alteration of the Authorization requirement for this activity?

In the Privacy Rule, creating de-identified data or a limited data set is a health care operation of the covered entity and, thus, does not require the covered entity to obtain an individual's Authorization or a waiver of the Authorization requirement, even if the limited data set or de-identified data will function as a research database. However, if a business associate is hired by a covered entity to create de-identified data or a limited data set, such activity must be conducted in accordance with the business associate requirements at sections 164.502(e) and 164.504(e).

A covered entity's subsequent disclosure of a limited data set–in any form, including as a database–for research must be made pursuant to a data use agreement between the covered entity and the recipient of the limited data set.

Objectives

1. To Provide an Overview of HIPAA Privacy Requirements That Impact Research
2. To Discuss How HIPAA Differs From Human Research Protection (i.e. IRB) Regulations
3. To Share a Select List of Frequently Asked Questions Regarding Research & HIPAA

References

- Research Repositories, Databases, and the HIPAA Privacy Rule http://privacyruleandresearch.nih.gov/research_repositories.asp
- Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule http://privacyruleandresearch.nih.gov/pr_02.asp
- Health Services Research and the HIPAA Privacy Rule http://privacyruleandresearch.nih.gov/healthservicesprivacy.asp

References

- Clinical Research and the HIPAA Privacy Rule http://privacyruleandresearch.nih.gov/clin_research.asp
- Institutional Review Boards and the HIPAA Privacy Rule http://privacyruleandresearch.nih.gov/irbandprivacyrule.asp
- Johns Hopkins HIPAA Questions and Answers Relating to Research http://www.hopkinsmedicine.org/institutional_review_board/hipaa_research/faq_research.html

University of Kentucky
HIPAA Authorization Template

Authorization to Create, Access, Use and Disclose Protected Health Information for Research Purposes

[Note: Information in the Authorization should NOT conflict with the consent form.]

The privacy law, HIPAA (Health Insurance Portability and Accountability Act), requires researchers to protect your health information. This form describes how researchers may use your information. Please read it carefully.

Your health information will be used and/or released (disclosed) for the following research study: [*Insert title of study*].

You allow (or authorize) [*name of researcher*] and *[his/her]* research staff at the University of Kentucky to create, access, use and release your health information for the purposes listed below.

The privacy law, HIPAA (Health Insurance Portability and Accountability Act), requires researchers to protect your health information. The following sections of the form describe how researchers may use your health information.

Your health information that may be accessed, used and/or released includes:

- (*List all of the protected health information[*] to be collected for this protocol/study such as demographic information, results of physical exams, blood tests, X-rays, and other diagnostic and medical procedures as well as medical history. Also include Medicare Health Insurance Claim Numbers (HICN), Social Security Numbers (SSN) and Employer Identification Numbers (EIN) if regulated by Medicare reporting provisions)*

Your health information will be used for:

- [*Provide a brief description of **each** research project or paste information from purpose section in the consent form; indicate that PHI is necessary to conduct the research, and meet legal, institutional and accreditation requirements*]

The Researchers may use and share your health information with:

(*Note: The information listed in this section should include all the agencies/researchers included in the consent form; however, the authorization may require additional information or more specific information than the consent form.)*

- The University of Kentucky's Institutional Review Board/Office of Research Integrity.
- Law enforcement agencies when required by law.

[*] Name, Address, Dates Directly Related to an Individual, Telephone/Fax Number, E-mail/Internet Protocol or Web URL Address, Social Security Number, Medical Record or Health Plan Number, Account Number, Certificate of License Number, Photographic Images, Vehicle Identifiers, Device Identifiers, Biometric Identifiers, Any Other Unique Code

- University of Kentucky representatives.
- *(UK Hospital if applicable. You must include this item if you are providing financial compensation for study participation or obtaining lab results from UKMC.)*
- *(If your research fall under the purview of a government agency (i.e., FDA, NIH, etc) list them in this section of the authorization form.)*
- (*Investigational Drug Service (IDS) if investigational drugs are dispensed through IDS.)*
- *(Center for Clinical and Translational Science (CCTS) if CCTS staff are involved in the study.)*
- *(List any collaborators, outside laboratories, etc.)*
- *(If applicable – list the sponsor's name and its agent(s) or government agency funding your research.)*
- *(List any other groups with whom the information may be shared.)*
- *(If applicable - statement that primary physician will be contacted if researcher in the course of the project learns of a medical condition that needs immediate attention.*)

The researchers agree to only share your health information with the people listed in this document.

Should your health information be released to anyone that is not regulated by the privacy law, your health information may be shared with others without your permission; however, the use of your health information would still be regulated by applicable federal and state laws.

You (*insert may or wil)]* not be allowed to participate in the research study if you do not sign this form. If you decide not to sign the form, it will not affect your:

- **Current or future healthcare at the University of Kentucky**
- **Current or future payments to the University of Kentucky**
- **Ability to enroll in any health plans (if applicable)**
- **Eligibility for benefits (if applicable)**

After signing the form, you can change your mind and NOT let the researcher(s) release or use your health information (revoke the Authorization). If you revoke the authorization:

- You will send a written letter to: (*name and contact information)* to inform *(him/her)* of your decision.
- Researchers may use and release your health information **already** collected for this research study.
- Your protected health information may still be used and released should you have a bad reaction (adverse event).
- You may not be allowed to participate in the study.

[Optional item: You understand that you will not be allowed to review the information collected for this research study until after the study is completed. When the study is over, you will have the right to access the information.]

The use and sharing of your information has no time limit.

If you have not already received a copy of the Privacy Notice, you may request one. If you have any questions about your privacy rights, you should contact the University of Kentucky's Privacy Officer at: (859) 323-1184.

You are the subject or are authorized to act on behalf of the subject. You have read this information, and you will receive a copy of this form after it is signed.

When developing the authorization form, please format to ensure the signature lines fall on a page containing text.

_____	_____
Signature of research subject or *research subject's legal representative	Date
_____	_____
Printed name of research subject or *research subject's legal representative	Representative's relationship to research subject

*(*If, applicable)* Please explain Representative's relationship to subject and include a description of Representative's authority to act on behalf of subject:

_____

_____

"Form K"

University Of Kentucky
HIPAA Waiver of Authorization Form

1. The use or disclosure of Protected Health Information (PHI)* involves no more than a minimal risk to the privacy of individuals. Explain why.

_____
_____
_____

2. Include a detailed list of the PHI to be collected and a list of the source(s) of the PHI.

_____
_____
_____

3. Describe the plan to protect PHI.

_____
_____
_____

4. Indicate where PHI will be stored.

_____
_____
_____

5. Who will have access to the PHI? (Note: researchers must list all of the entities that are able access to the study's PHI such as Office of Research Integrity/Institutional Review Board, UK/Hospital representatives, sponsors, FDA, data safety monitoring boards and any others given authority by law).

_____
_____

6. All PHI collected during the study will be destroyed at the earliest opportunity consistent with the conduct of research, which is: (explain below). Alternatively, PHI collected during the study will not be destroyed because: (explain below).

_____
_____

7. Please describe the procedure used to destroy PHI collected during the study (electronically, paper, audio/video, photography, other).

_____
_____
_____

8. The research could not practicably be conducted without the waiver because (explain below).

_____
_____
_____

9. The research could not practicably be conducted without access to and use of the PHI because (explain).

_____
_____
_____

10. The HIPAA regulation requires reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Please note that researchers are also accountable for any PHI released under a waiver. Explain why PHI obtained for this study is/are the minimum information needed to meet the research objectives.

_____
_____
_____

The information listed in the waiver application is accurate and all research staff** will comply with the HIPAA regulations and the waiver criteria. I assure that PHI obtained as part of this research will not be reused or disclosed to any other person or entity other than those listed on this form, except as required by law. If at any time I want to reuse this information for other purposes or disclose the information to other individuals or entity I will seek approval by the IRB.

Investigator's Name:_____ Date:_____

Principal Investigator Signature: _____

*PHI: individually identifiable health information transmitted or maintained in any form (electronic means, on paper, or through oral communication) that relates to the past, present or future physical or mental health or conditions of an individual plus any of the 18 identifiers listed in the regulations.
**Note: Research staff is defined as ALL study personnel (including PI) that is involved in the research.

EP-00006

HIPAA IRB Form 8.4,
(Revised 12/1/12)

TRACKING FORM FOR PERMITTED GENERAL DISCLOSURES OF PHI FROM CLINICAL OR RESEARCH RECORDS

Regulations issued under the Health Insurance Portability and Accountability Act ("HIPAA") require Johns Hopkins to make a written record of disclosures of individually identifiable health information that John Hopkins makes in the situations listed at the bottom of this form. A disclosure is sharing PHI with someone outside the Johns Hopkins covered entities. Use this form to keep a record of each disclosure made about an individual.

Individual's Name: _____

Individual's Medical Record Number: _____
or
Study title and study number: _____

Person Making the Disclosure: _____

Part I

Date	Name of Person/Entity Who Received Health Information and Address (if known)	Brief Description of Health Information Disclosed	Brief Statement of the Purpose of the Disclosure (List the category number from below plus specific purpose)

HIPAA Tracking Requirements

1. Disclosures Required by Law
2. Disclosures for Public Health Activities
3. Disclosures About Victims of Abuse or Neglect of Children or Vulnerable Adults
4. Disclosures for Health Oversight Activities
5. Disclosures for Judicial and Administrative Proceedings (subpoenas, court orders, etc.)
6. Disclosures for Law Enforcement Purposes
7. Disclosures About Decedents to Medical Examiners and Funeral Directors
8. Disclosures for Organ and Transplant Donation Purposes
9. Disclosures to Avert a Serious Threat to Health or Safety
10. Disclosures for Specialized Government Functions
11. Disclosures to the Secretary of the U.S. Dept. of Health & Human Services
12. Disclosures from Clinical Records to Non-Johns Hopkins Researchers

Part II

The following portion of this form should be used when you make multiple disclosures of PHI about the same individual to the same person or entity in any of the situations listed above. For example, use the following portion of this form if you make periodic disclosures to the same recipient regarding the same incident of abuse or neglect or if you review a study participant's records and make ten disclosures to health regulatory agency "x" over time about the same study participant. Fill in complete information about the individual for the first disclosure to the recipient and then only the information requested below for the subsequent disclosures about the individual to the same recipient. Complete this form for each individual for whom you make multiple disclosures to the same person or entity.

For Each Subsequent Disclosure to the Same Recipient About the Same Individual, Record the Following:

1. Individual: _____
2. The name of the entity or person who received the PHI: _____
   _____
3. The date or frequency of the disclosure: _____
   _____
4. Name of the person making the disclosure: _____

Part I of this form must be filled out and submitted after the first disclosure about the individual is made. Part II of this form must be filled out and submitted after each subsequent disclosure about the individual to the same recipient is made.

NOTE: 1. If the disclosure is made from the **clinical records**, submit this form to the Medical Records Department.

2. If the disclosure is made from **research records**, submit this form to the HIPAA Privacy Officer each time you make a disclosure by e-mail to HIPAA@jhmi.edu or by sending a written notice to:

Johns Hopkins Privacy Officer
5801 Smith Avenue
McAuley Hall, Suite 310
Baltimore, MD 21209
Fax 410-735-6521

.

Frequently Asked Questions

1. How is the HIPAA Privacy Rule related to the HIPAA Security Rule?

2. I am a researcher who has obtained a Certificate of Confidentiality for my study. Do I need a HIPAA Privacy Authorization when I already have a Certificate of Confidentiality?

3. A researcher requests data that assigns a code derived from the last four digits of the social security number. This code is necessary to link individual records from different data sources. The data contain none of the other listed HIPAA identifiers at section 164.514(b)(2). Are the data de-identified under the Privacy Rule?

4. Are an individual's initials considered to be identifiers under the Privacy Rule?

5. How does the Privacy Rule apply to research involving blood or tissue samples?

6. I am a health services researcher employed by a university that has designated itself as a “hybrid entity” for purposes of the Privacy Rule. The university’s hospital and medical school are within the “health care component” of the hybrid entity, but my epidemiology department is not. Am I subject to the Privacy Rule requirements that apply to the health care component of the university?

7. I am conducting a large research study in which I will obtain data from multiple covered entities. Must each covered entity disclosing data to me for my research receive documentation that its own IRB or Privacy Board has granted my project a waiver of Authorization?

8. May a covered entity that performs research create de-identified health information to be used to prepare a grant application for research as part of its health care operations, or is this activity a review preparatory to research?

9. Is a covered entity’s patient list that includes only names and addresses considered to be PHI if there is no other health or payment information attached?

10. May a covered entity rely on an Authorization signed by parent on behalf of a minor child, even after the child has reached the age of majority? Similarly, would the Privacy Rule’s transition provisions “grandfather” an informed consent signed by a minor’s parent even if the child reached the age of majority before the Privacy Rule compliance date?

11. Does the Privacy Rule permit a researcher who is a covered workforce member of a covered entity to transfer PHI, without individual Authorization, to another institution if, for example, the researcher changes jobs?

12. When might I need a HIPAA Data Use Agreement in connection with my research?

13. What is a limited data set, and what are its advantages?

14. What types of information (direct identifiers) must be omitted from PHI in order to qualify the information as a limited data set?

15. May a limited data set include the geographic subdivision code with the five-digit ZIP code (or a nine-digit ZIP code)?

16. What is the difference between a de-identified data set and a limited data set?

17. May a limited data set include a unique code or identifier not listed at section 164.514(e)(2) of the Privacy Rule?

18. I work for a covered entity and conduct observational studies on patients' reactions to various emergency room triaging. The nature of the study requires that individuals not know they are being observed. Under HHS Protection of Human Subjects Regulations, the IRB is allowed to waive the informed consent requirement when certain criteria are met. Must I also receive documentation of an IRB waiver of the Authorization requirement under the Privacy Rule for observational studies?

19. Does a covered entity need to account for disclosures of PHI contained in a limited data set?

20. At what point in recruitment may we gather information about a potential participant (i.e., a potential participant calls our office after seeing a flier, may we screen that person/ ask them about their history, or do we need him or her to complete a written privacy Authorization prior to screening)?

21. When a potential participant calls after seeing a flier, may we take a history from the participant to determine eligibility prior to receiving a written privacy Authorization if we do not record (either in a database or written form) the PHI given to us by the participant?

22. When the potential participant calls our office, may the staff member who took the call have another staff member (same research team) send materials to/contact the potential participant?

23. May a covered health care provider discuss with a patient his or her enrollment in clinical research without the patient's Authorization? What if the individual is not a patient of the covered provider?

24. May a covered entity obtain an individual's Authorization to include his or her PHI in a clinical research recruitment database of possible research participants, such as a pre-screening log?

25. One common method for recruiting research participants involves organizing a call center for potential research participants to contact in response to advertisements about the research. Would a call center be required to obtain the individual's Authorization before speaking to the individual about the trial?

26. May a covered entity use or disclose PHI to locate or identify the whereabouts of a research participant (e.g., subjects who are "lost to follow-up")?

27. I am a researcher, and my research data source is asking me to sign a business associate agreement. Is this necessary?

28. Do the HIPAA requirements allow for participants to request a copy of any structured interviews they completed/responded to as part of the study? What about the results of research laboratory tests?

29. I am enrolling subjects in a clinical study. If adverse events occur and my subjects are treated by another provider, how may I obtain information about the subjects' treatment?

30. If, under the "preparatory to research" provisions, a researcher identifies subjects that meet the study's eligibility criteria, how can the researcher contact the potential participant to obtain Authorization after identifying these individuals?

31. May a covered entity hire a researcher as a business associate to de-identify health information when the researcher is the intended recipient of the de-identified data?

32. May a covered entity that has hired a researcher as its business associate for the purposes of de-identifying data permit the researcher to assign to the de-identified data a re-identification code, if the researcher is also the intended recipient of the de-identified data?

33. Is a covered entity permitted, as part of its health care operations activities, to disclose PHI to a business associate to create de-identified data or a limited data set that may function as a research database? Or does the covered entity need an Authorization or a waiver or alteration of the Authorization requirement for this activity?