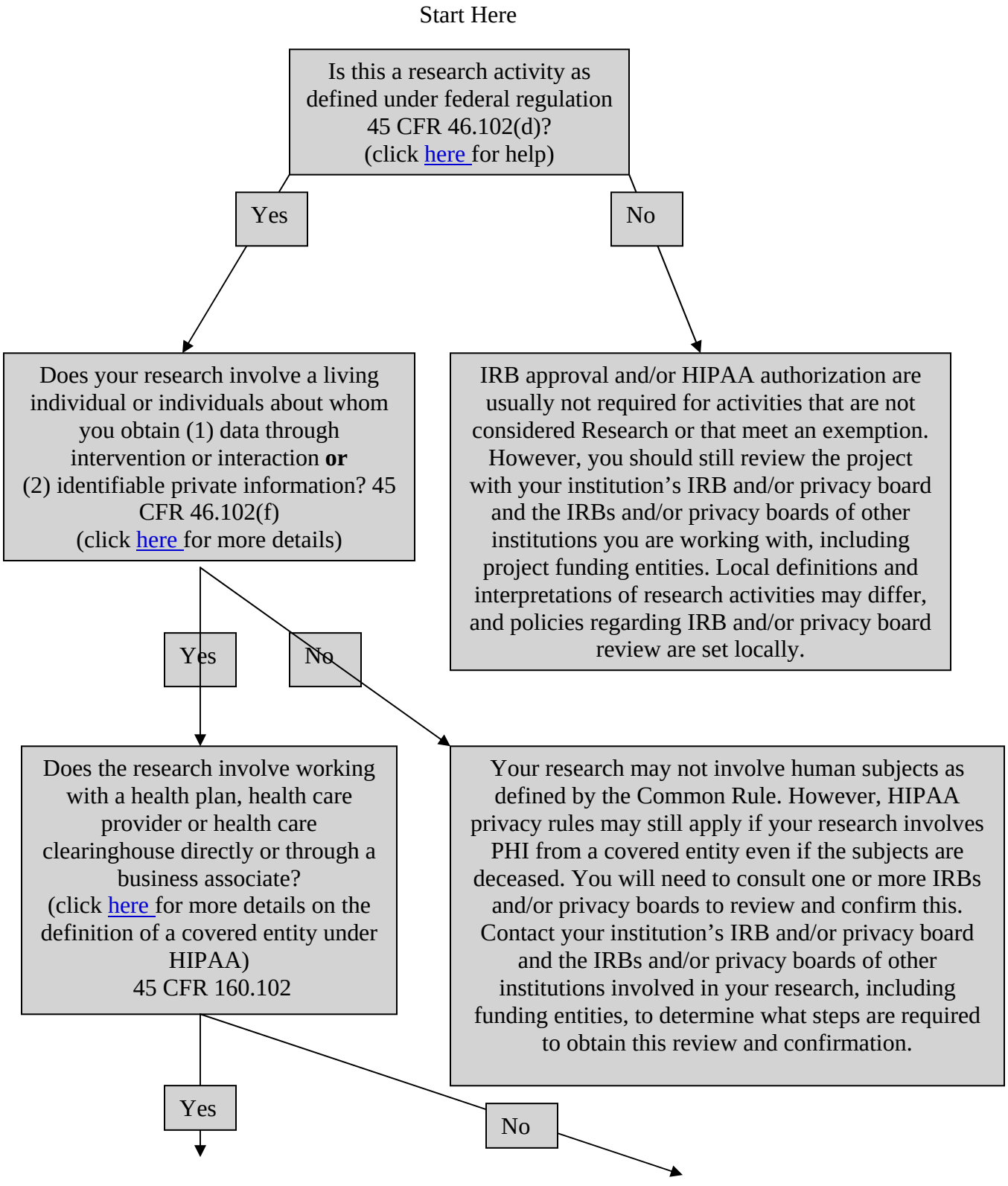
HIPAA and Privacy: Resources for HSR

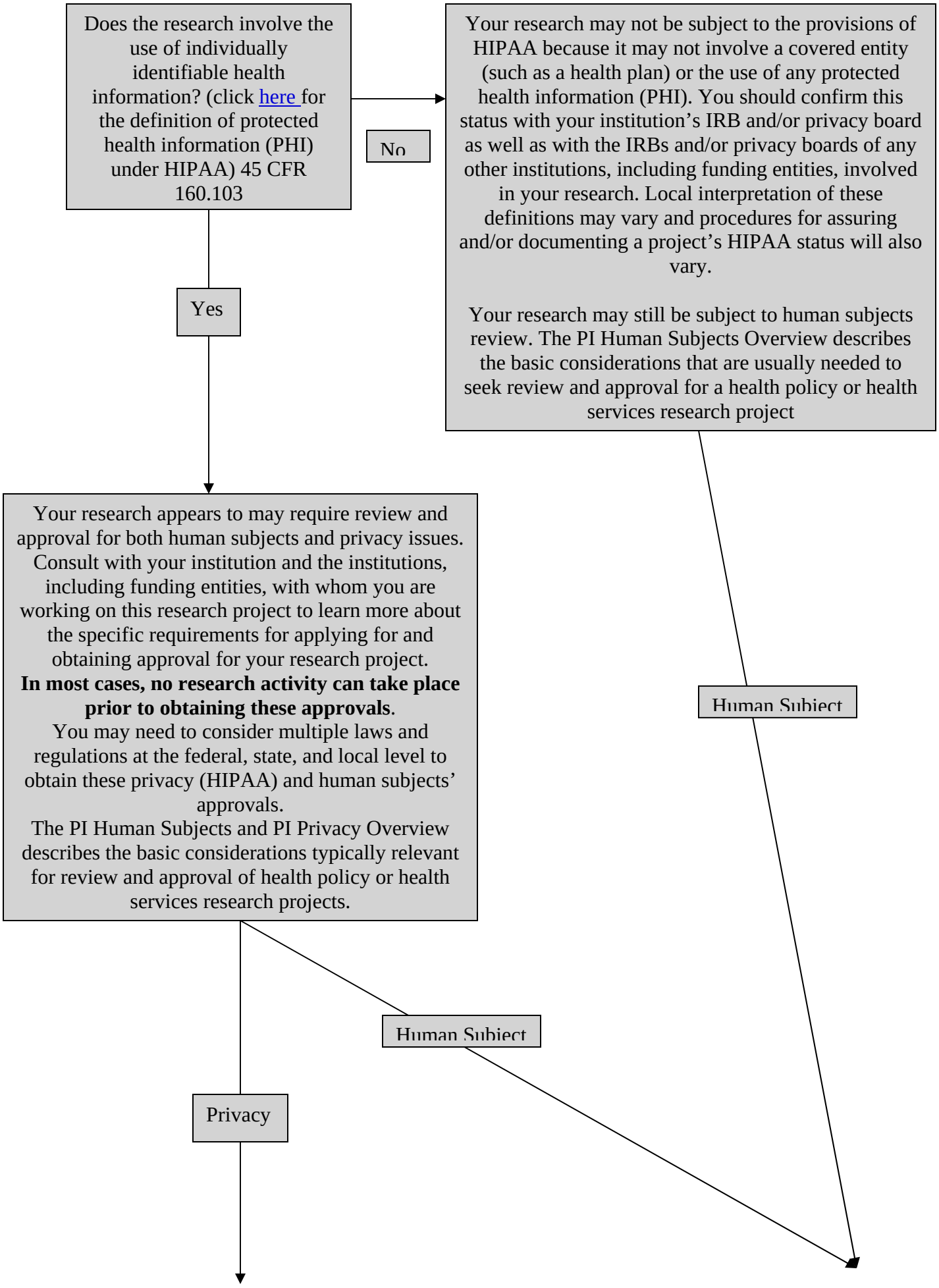
Don Steinwachs and Hal Luft

AcademyHealth

Interactive Guide to Finding if Your Research Project May be Affected by the HIPAA Privacy Rule or the Common Rule

This Guide is intended to help you find if your research project is impacted by the HIPAA Privacy Rule or the Common Rule. This is not a substitute for reviewing the rules, consulting funding agencies and Institutional Review Boards, or obtaining legal advice.




Does the research involve the use of individually identifiable health information? (click here for the definition of protected health information (PHI) under HIPAA) 45 CFR 160.103
No
Your research may not be subject to the provisions of HIPAA because it may not involve a covered entity (such as a health plan) or the use of any protected health information (PHI). You should confirm this status with your institution's IRB and/or privacy board as well as with the IRBs and/or privacy boards of any other institutions, including funding entities, involved in your research. Local interpretation of these definitions may vary and procedures for assuring and/or documenting a project's HIPAA status will also vary.
Your research may still be subject to human subjects review. The PI Human Subjects Overview describes the basic considerations that are usually needed to seek review and approval for a health policy or health services research project
Yes
Your research appears to may require review and approval for both human subjects and privacy issues. Consult with your institution and the institutions, including funding entities, with whom you are working on this research project to learn more about the specific requirements for applying for and obtaining approval for your research project.
In most cases, no research activity can take place prior to obtaining these approvals.
You may need to consider multiple laws and regulations at the federal, state, and local level to obtain these privacy (HIPAA) and human subjects' approvals.
The PI Human Subjects and PI Privacy Overview describes the basic considerations typically relevant for review and approval of health policy or health services research projects.
Human Subject
Human Subject
Privacy

HIPAA Privacy Rule Considerations for Obtaining and Using Privacy Health Information

Overview: Principal Investigators ("**PI**") seeking access to and use of Private Health Information ("**PHI**") of individually identifiable persons need to understand how the HIPAA[1] Privacy Rule affects their access to and use of such information. The following information is provided to assist PI identification of issues they may have to consider in accessing and using such information. Additional guidance may be obtained at http://www.hhs.gov/ocr/hipaa/ and http://www.hhs.gov/ocr/privacysummary.pdf. In addition to considering the HIPAA Privacy Rule, PIs must also identify and comply with any additional federal, state, local, or institutional or funding agency privacy regulations or policies.

Some HIPAA Terminology

The Privacy Rule: The US Department of Health and Human Services issued the Privacy Rule in accordance with HIPAA. The Privacy Rule addresses the use and disclosure of individuals' health information (called Protected Health Information or PHI) by organizations subject to the Privacy Rule (called Covered Entities). The Privacy Rule requires that research subjects give *authorization* (contrast with human subject *consent* to participate in research) to use their PHI. Under some limited circumstances as defined within the regulation, individual authorization for PHI may be waived.

Business Associate: A business associate is generally an organization that performs functions or services for a covered entity that involve the use or disclosure of individually identifiable health information. These functions and services may include, but are not limited to, claims processing, data analysis, utilization review, and billing. Health policy and services researchers will oftentimes *not* need a business associate contract with a covered entity, but rather a protocol approved by an IRB or privacy board that meets HIPAA privacy rule requirements (see below). However, covered entities may initially assume that a business associate relationship is required before they can allow health policy or services research using PHI.

Covered Entities: health plans, health care clearinghouse, a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule. Decision tool for covered entity status found at www.hhs.gov/oc/hipaa

Privacy Boards: For many health policy and services research projects, it is not practicable to obtain individual authorization to use PHI from all research subjects. Privacy boards, as well as IRBs, may consider and grant a request to waive (or alter) research subject authorization to use PHI. Covered entities may have an IRB, a privacy board, or both. PI's seeking a waiver or alteration of authorization must determine to whom to make their request.

Protected Health Information: means individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

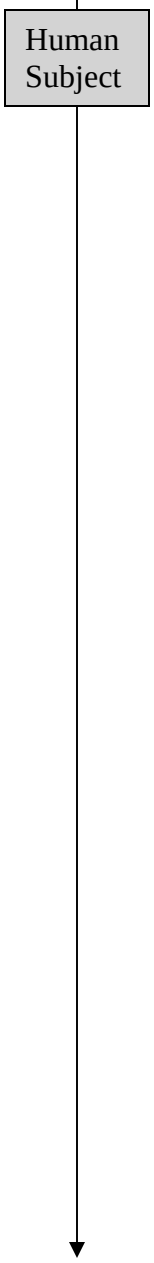
Protected Health Information (PHI), HIPAA, and Research

Overview: PHI includes demographic and other data that relates to a specifically identifiable individual's past, present or future physical or mental health or condition; the provision of health care to that individual; or the past, present, or future payment for the provision of health care to that individual.

Authorized Use of PHI: Individuals may authorize in writing the release and/or disclosure of their PHI by covered entities. Health policy and services researchers who directly interact with subjects may obtain this authorization. Subjects can often provide authorization at the same time as informed consent.

De-identifying Health Information: PI's may chose to conduct research with de-identified health information. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of 18 specified identifiers the absence of any knowledge by the covered entity that the remaining information could be used to identify the individual. Researchers must consult with the relevant privacy boards and IRBs to determine which of these two approaches should be used for their particular research project.

Disclosing PHI for Research: The Privacy Rule permits a covered entity to use and disclose PHI without written authorization by the subject of the PHI for research in the limited circumstances where the covered entity obtains: (1) documentation that alteration or waiver of individual authorizations has been approved by an IRB or Privacy Board; (2) representation by the researcher that the only intended use of the information is to prepare a research protocol for which the PHI is necessary for the research with an assurance that no PHI will be removed from the covered entity; and (3) if the research is solely for examining PHI of deceased persons and is necessary for the research. Covered entities also may make de-identified datasets available for health policy and services research.



Human Subjects Guidelines

Overview: This document identifies the basic considerations relevant to obtain human subject approvals for a research project. Many of these elements derive from the US Federal Common Rule (45 CFR 46). Principle Investigators (PIs) ***must*** identify how Common Rule provisions are implemented and interpreted by local institutions and research partners. Researchers must also identify any additional federal, state, local, or institutional human subjects protection regulations or policies that may apply. Researchers should also consult with funders to determine their requirements for human subjects' protection.

Institutional Review Board (IRB)

Overview: An IRB conforming to Federal regulations, State laws, and institutional policy, reviews research proposals involving human subjects to promote the ethical and equitable treatment of those subjects. Representatives of your research institution can direct you to the appropriate IRB. IRB approval is generally required for all human subjects' research.

Informed Consent

Overview: PIs must develop procedures, protocols, and justifications for obtaining informed consent from research subjects. Generally, this includes written consent:

1. outlining the procedures for **obtaining informed consent** from research subjects
2. developing a protocol for **documenting informed consent** from research subjects
3. justifying the procedures and protocols in the context of the overall research project.

Your IRB and the IRBs of the institutions you are working with (including funding entities) will determine the specific procedures and protocols that are appropriate for your particular research project.

Written, Oral, and Waiver
Health policy and services researchers may seek written, oral, or waiver of informed consent and informed consent documentation. The propriety of written versus oral consent often depends on the research protocol, as detailed in table 1 below.

Table 1: Methods of obtaining and documenting informed consent

Purpose	*Secondary Data Analysis or Analysis of Administrative Data*	*Telephone Interview or Survey*	*In-Person Interview or Survey*	*Direct Observation or Ethnography*
Written	Difficult to obtain unless done at the time of original interaction	Usually not feasible	Usually required	Usually not required
Oral	Usually not considered adequate. Often not feasible	Often considered adequate. Obtain before starting interview	Possible in some very low risk projects.	Usual practice
Waiver	May be considered adequate. Consult PI Privacy Checklist for further information.	Usually not considered adequate.	Usually not considered adequate.	May be considered adequate, especially for observations in public setting

Confidentiality

Overview: Health policy and services research may put subjects at risk of a loss of confidentiality of information they or HIPAA would deem private. Your IRB and the IRBs of the institutions with which you are working (including funding entities) will determine the specific procedures and protocols that are considered adequate for protecting subject confidentiality. There are some general principles that health policy and services researchers should consider to protect subject confidentiality as well as some specific steps that can be taken depending on the research design, as detailed in table 2 below.

Table 2: Preserving research subject confidentiality

Secondary Data Analysis or Analysis of Administrative Data	*Telephone Interview or Survey*	*In-Person Interview or Survey*	*Direct Observation or Ethnography*
Consult PI Privacy Checklist	1. separate individual identifiers from data in paper and electronic files 2. withhold identifying details of individuals and study sites in public reports and documents 3. destroy documents with individually-identified information as soon as possible	1. separate individual identifiers from data in paper and electronic files 2. withhold identifying details of individuals and study sites in public reports and documents 3. destroy documents with individually-identified information as soon as possible	1. use pseudonyms in field notes 2. don't reveal location of study sites 3. alter and/or withhold identifying details of individuals and study sites in public reports and documents 4. destroy primary documents if possible
1. maintain electronic records in password protected documents and computers 2. keep electronic files on secure computer networks 3. keep paper files in locked cabinets and offices 4. restrict file access to study team			

Risks

Overview: Research subjects' perception of risk may vary, and subjects may experience health policy or services research as intrusive or invasive. In the context of the Common Rule, some IRBs may consider many health policy or services research projects to be "minimal risk", i.e. not exceeding those encountered in everyday life (See CFR 46.102(i)). However, PIs can not assume that their research is minimal risk and must consult with their IRB.

The risks of most health policy or services research:

1. includes potential loss of confidentiality;
2. may include potential for embarrassment due to answering personal questions.

Steps to address and minimize these risks may include:

1. instituting appropriate measures to guard confidentiality and privacy (see table above);
2. informing subject that participating will not affect their medical care;
3. allowing respondent to terminate participation at any time.

Benefits

Usually there are no direct benefits to subjects from participating in a health policy or services research project. Usually there are some benefits to society at large due to new research knowledge.

Special Populations

Certain classes of subjects including **minors, prisoners, pregnant women, human fetuses, neonates,** and **those unable to consent to research participation on their own** benefit from special protections when it comes to health policy or services research. If your research project involves any of these special populations, you should consult with your IRB to learn how to include adequate human subject protections for these special populations.

HIPAA: Data Use Agreement

Derived from HIPAA Regulation Section 164.514 (e)

I. What is a Data Use Agreement (DUA)?

- A covered entity may use or disclose a "limited data set" if that entity obtains a data use agreement from the potential recipient; in our case, the health services researcher. 164.514 (e) (1)

- This information can only be used for:
  - Research;
  - Public health; or
  - Health care operations.

  164.514 (e) (3) (I)

- A limited data set is protected health information that **excludes** the following direct identifiers of the individual or of relatives, employers, or household members of the individual: 164.514 (e) (2)

  - Names;
  - Postal address information, *except* town or city, State, and zip code;
  - Telephone numbers;
  - Fax numbers;
  - Email Addresses;
  - Social Security Numbers;
  - Medical record numbers;
  - Health plan beneficiary numbers;
  - Account numbers;
  - Certificate/ license numbers;
  - Vehicle identifiers and serial number, including license plate numbers;
  - Web URL's;
  - IP addresses;
  - Biometric identifiers, including finger and voice prints; and
  - Full face photographic images and any comparable images.

II: What must be in a DUA?

164.514 (e) (4) (ii)

- A DUA must do the following:
  - Establish what the data will be used for, as permitted above. The DUA must not violate this principle.
  - Establish who is permitted to use or receive the limited data set.
  - Provide that the limited data set recipient will:
    - Not use the information in a matter inconsistent with the DUA or other laws.
    - Employ safeguards to ensure that this does not happen.

- Report to the covered entity any use of the information that was not stipulated in the DUA.
- Ensure that any other parties, including subcontractors, agree to the same conditions as the limited data set recipient in the DUA.
- Not identify the information or contact the individuals themselves.

A covered entity is **not** in compliance with the regulation if: 164.514 (e) (4) (iii) (A)

- The entity knew of a pattern of activity by the limited data set recipient that violates the DUA unless they attempted to resolve the violation. The measures they must take are to:
  - Discontinue disclosure of the protected health information to the recipient; and
  - Report the problem to the Secretary.

III: What Does a DUA Look Like?

Model Data Use Agreement:

Adapted from Washington University:
http://medicine.wustl.edu/~hsc/hipaa/Datauseagreementexternal.rtf

FOR EXTERNAL USE ONLY

DATA USE AGREEMENT

This Data Use Agreement ("Agreement") is made and entered into as of this _____ day of _____, 20__ by _____("Covered Entity"), and _____ ("Data Recipient").

WITNESSETH:

WHEREAS, Covered Entity may Disclose or make available to Data Recipient, and Data Recipient may Use, Disclose, receive, transmit, maintain or create from, certain information in conjunction with research; and

WHEREAS, Covered Entity and Data Recipient are committed to compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and regulations promulgated thereunder; and

WHEREAS, the purpose of this Agreement is to satisfy the obligations of Covered Entity under HIPAA and to ensure the integrity and confidentiality of certain information Disclosed or make available to Data Recipient and certain information that Data Recipient Uses, Discloses, receives, transmits, maintains or creates, from Covered Entity.

NOW, THEREFORE, in consideration of the foregoing recitals and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

A. DEFINITIONS

Terns used but not otherwise defined in this Agreement shall have the same meaning as those terms in the Privacy Rule.

1. Individual shall have the same meaning as the term "individual" in 45 CFR Sect. 164.501 of the Privacy Rule and shall include a person who qualifies as a personal representative in accordance with 45 CFR Sect. 164.502(g) of the Privacy Rule.

2. Limited Data Set shall have the same meaning as the term "limited data set" in 45 CFR 164.514(e) of the Privacy Rule.

3. Privacy Rule shall mean the Standards for Privacy of Individually Identifiable Information at 45 CFR Part 160 and Part 164, Subparts A and E, as amended from time to time.

4. Protected Health Information or PHI shall have the same meaning as the term "protected health information" in 45 CFR Sect. 164.501 of the Privacy Rule, to the extent such information is created or received by Data Recipient from Covered Entity.

5. Required by Law shall have the same meaning as the term "required by law" in 45 CFR Sect. 164.501 of the Privacy Rule.

B. SCOPE AND PURPOSE

1. This Agreement sets forth the terms and conditions pursuant to which Covered Entity will Disclose certain PHI to the Data Recipient.

2. Except as otherwise specified herein, Data Recipient may make all Uses and Disclosures of the Limited Data Set necessary to conduct the research described herein: _____(include a brief description of the research and/or HSC protocol number)_____ ("Research Project").

3. In addition to the Data Recipient, the individuals, or classes of individuals, who are permitted to Use or receive the Limited Data Set for purposes of the Research Project, include: _____
_____.

C. OBLIGATIONS AND ACTIVITIES OF DATA RECIPIENT

164.514 (e)(4)(ii)(A)

1. Data Recipient agrees to not Use or Disclose the Limited Data Set for any purpose other than the Research Project or as Required by Law. 164.514 (e)(4)(ii)(C)(1)

2. Data Recipient agrees to use appropriate safeguards to prevent Use or Disclosure of the Limited Data Set other than as provided for by this Agreement. 164.514 (e)(4)(ii)(C)(2)

3. Data Recipient agrees to report to the Covered Entity any Use or Disclosure of the Limited Data Set not provided for by this Agreement of which it becomes aware, including without limitation, any Disclosure of PHI to an unauthorized subcontractor, *within ten (10) days of its discovery (optional)*. 164.514 (e)(4)(ii)(C)(3)

4. Data Recipient agrees to ensure that any agent, including a subcontractor, to whom it provides the Limited Data Set agrees to the same restrictions and conditions that apply through this Agreement to the Data Recipient with respect to such information. 164.514 (e)(4)(ii)(C)(4)

5. Data Recipient agrees not to identify the information contained in the Limited Data Set or contact the individual. 164.514 (e)(4)(ii)(C)(5)

6. Data Recipient will indemnify, defend and hold harmless Covered Entity and any of Covered Entity's affiliates, and their respective trustees, officers, directors, employees and agents ("Indemnities") from and against any claim, cause of action, liability, damage, cost or expense (including, without limitation, reasonable attorney's fees and court costs) arising out of or in connection with any unauthorized or prohibited Use or Disclosure of the Limited Data Set or any other breach of this Agreement by Data Recipient or any subcontractor, agent or person under Data Recipient's control. (optional)

D. TERM AND TERMINATION

The provisions of this Agreement shall be effective as of the earlier of Effective Date or April 14, 2003 and shall terminate when all of the Limited Data Set provided by Covered Entity to Data Recipient is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy the Limited Data Set, protections are extended to such information, in accordance with the termination provisions in this Section.

E. MISCELLANEOUS

1. A reference in this Agreement to a section in the Privacy Rule means the section as amended or as renumbered.

2. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and HIPAA.

3. The respective rights and obligations of Data Recipient under Section C of this Agreement shall survive termination of this Agreement.

4. Any ambiguity in this Agreement shall be resolved to permit Covered

Entity to comply with the Privacy Rule.

5. There are no intended third party beneficiaries to this Agreement. Without in any way limiting the foregoing, it is the parties' specific intent that nothing contained in this Agreement gives rise to any right or cause of action, contractual or otherwise, in or on behalf of the individuals whose PHI is Used or Disclosed pursuant to this Agreement.

6. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.

7. The persons signing below have the right and authority to execute this Agreement and no further approvals are necessary to create a binding agreement.

8. In the event of any conflict between the terms and conditions stated within this Agreement and those contained within any other agreement or understanding between the parties, written, oral or implied, the terms of this Agreement shall govern. Without limiting the foregoing, no provision of any other agreement or understanding between the parties limiting the liability of Data Recipient to Covered Entity shall apply to the breach of any covenant in this Agreement by Data Recipient.

9. This Agreement shall be construed in accordance with and governed the laws of the state or jurisdiction of the covered entity

IN WITNESS WHEREOF, the parties have executed this Agreement effective upon the Effective Date set forth above.

COVERED ENTITY	DATA RECIPIENT
Name:_____	Name:_____
Title: _____	Title:_____

HIPAA: Individual Authorizations

I: What is an Individual Authorization?

Adapted from the Health and Human Services' Office of Civil Rights
http://www.hhs.gov/ocr/hipaa/

Research Use/Disclosure with Individual Authorization. The Privacy Rule permits covered entities to use or disclose protected health information for research purposes when a research participant authorizes the use or disclosure of information about him or herself. Today, for example, a research participant's authorization will typically be sought for most clinical trials and some records research. **In this case, documentation of IRB or Privacy Board approval of a waiver of authorization is not required for the use or disclosure of protected health information.**

Some Researcher-Specific Points:

To use or disclose protected health information with authorization by the research participant, the covered entity must obtain an authorization that satisfies the requirements of 45 CFR 164.508. The Privacy Rule has a general set of authorization requirements that apply to all uses and disclosures, including those for research purposes. However, several special provisions apply to research authorizations:

I. Unlike other authorizations, an authorization for a research purpose may state that the authorization does not expire, that there is no expiration date or event, or that the authorization continues until the "end of the research study;" and

I. An authorization for the use or disclosure of protected health information for research may be combined with consent to participate in the research, or with any other legal permission related to the research study.

II: What must be in an Individual Authorization?

Model Individual Authorization

This document fully outlines the statements and the questions that must be answered in an individual authorization according to the new regulations.

This document may need to be modified, on a state-by-state basis, to comply with the provisions of applicable state law that are not preempted by HIPAA.

Derived from the American Society of Clinical Oncology: http://www.asco.org/ac/1,1003,_18-0022551-00_19-0022565-00_20-0010-00_12-002027,00.asp?ArticleId=22551&ArticleBodyId=22565&ShowHead=&PageNo=4&cancer_type_id=&state=

ASCO Document #9

Patient Name: _____

ID Number: _____

(Optional) *We understand that information about you and your health is personal, and we are committed to protecting the privacy of that information. Because of this commitment, we must obtain your special authorization before we may use or disclose your protected health information for the purposes described below. This form provides that authorization and helps us make sure that you are properly informed of how this information will be used or disclosed. Please read the information below carefully before signing this form.*

USE AND DISCLOSURE COVERED BY THIS AUTHORIZATION

A representative of the organization requesting the protected health information must answer these questions completely before providing this authorization form to you. DO NOT SIGN A BLANK FORM. You or your personal representative should read the descriptions below before signing this form.

Who will disclose the information? The person(s) or class of persons authorized to disclose the information is described below. 164.508 (c) (1) (iii)

_____

Who will use and/or receive the information? The person(s) or classes of persons authorized to use and/or receive the information are described below. 164.508 (c) (1) (ii)

_____

What information will be used or disclosed? The description below should be in enough detail so that you (or any organization that must disclose information pursuant to this authorization) can understand what information may be used or disclosed. 164.508 (c) (1) (i)

_____

What is the purpose of the use or disclosure? The purposes for which the information will be used or disclosed are described below. 164.508 (c) (1) (iv)

_____

When will this authorization expire?[1] The date or event that will trigger the expiration of this authorization should be described below. - See: "Some Researcher-Specific Points," and 164.508 (c) (1) (v)

_____

SPECIFIC UNDERSTANDINGS

By signing this authorization form, you authorize the use or disclosure of your protected health information as described above. This information may be redisclosed if the recipient(s) described on this form is not required by law to protect the privacy of the information. 164.508 (c) (2) (iii)

You have a right to refuse to sign this authorization. Your health care, the payment for your health care, and your health care benefits will not be affected if you do not sign this form.[2] 164.508 (c) (2) (ii) (A) and (B)

You have a right to see and copy the information described on this authorization form in accordance with our record access policies. You also have a right to receive a copy of this form after you have signed it. 164.508 (c) (4)

If you sign this authorization, you will have the right to revoke it at any time, except to the extent that we have already taken action based upon your authorization. To revoke this authorization, please write to [insert name of responsible person or department]. 164.508 (c) (1) (i)

SIGNATURE

164.508 (c) (1) (vi)

I have read this form and all of my questions about this form have been answered. By signing below, I acknowledge that I have read and accept all of the above.

_____
Signature of Patient or Personal Representative

_____
Print Name of Patient or Personal Representative

_____
Date

_____
Description of Personal Representative's Authority

CONTACT INFORMATION

The contact information of the patient or personal representative who signed this form should be filled in below.

Address:

_____

_____

_____

_____

Telephone:

_____ (daytime)

_____ (evening)

Email Address (optional):

_____

THE PATIENT OR HIS OR HER PERSONAL REPRESENTATIVE SHOULD BE PROVIDED WITH A COPY OF THIS FORM AFTER IT HAS BEEN SIGNED.

1 The covered entity should insert an expiration date, time period, or an event that will trigger expiration of the authorization. An expiration event must be related to the individual or the purpose(s) of the disclosure(s). For example, an authorization that expired on the date that the stock market reached a certain level would not be valid. *See* 65 Fed. Reg. 82,515. The statement "end of research study", "none" or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository. *See* HIPAA Privacy Regulation 164.508 (c)(1)(v)

2 When a covered entity is providing health care solely for the purpose of creating protected health information that will be disclosed to a third party, it may require that the individual sign the authorization form before providing the health care. *See* 45 C.F.R. 164.508(b)(4). A covered entity may modify this authorization form to apply to these situations by deleting this statement of understanding from the text of this form.

HIPAA: Institutional Review Boards and Privacy Boards

Adapted from HIPAA Privacy Regulation Section 164.512

I: When will you need to seek Institutional Review Board (IRB) or Privacy Board (PB) Approval?

A covered entity may use or disclose Protected Health Information (PHI) for research purposes, regardless of its funding source, as long as they obtain documentation from the researcher of board approval of a waiver or an alteration of an individual authorization. 164.512 (a)(1)

IRBs and PBs are independent entities that review research proposals to ensure that they meet the Federal government's regulations pertaining to the PHI of human subjects. These boards may also approve the authorization for a covered entity to release PHI to the researcher.

HIPAA requires that Privacy Boards:
164.512 (I)(1)(I)(B) (1-3)

- Have members from diverse backgrounds as well as the credentials and experience to evaluate a research proposal's impact on the individual's rights to privacy;
- Include at least one board member that has no affiliation with the covered entity, nor with any sponsoring entities of the research, and is not related to any person who falls under these criteria; and
- Does not have any member involved in a review of any project in which the member has a conflict of interest.

II: What will you need to present to the IRB/PB?

In order to prepare research protocol for IRB/PB approval, researchers may need access to PHI before their research begins. For this contingency, HIPAA requires that covered entities obtain the following written assurances from the prospective researcher:
164.512 (I)(1)(ii) (A-C)

- The researcher seeks the information only for the purposes of formulating research protocol, or other similar reasons of research preparation;
- No PHI will be removed from the covered entity while the researcher reviews that information; and
- The PHI that the researcher seeks is necessary for the purposes of their research.

If your proposal includes research on decedent's information, you must provide the covered entity with:
164.512 (I)(1)(iii)(A-C)

- Representation that the use or disclosure of the information is only for research on the PHI of decedents;
- Documentation of the death of those individuals, if the covered entity requests it; and

- Representation that the PHI is necessary for research purposes.

Before the research can begin, covered entities must receive documentation of the IRB/PB's waiver before they can release the PHI to the prospective researcher. This documentation must include these criteria:
164.512 (I)(2)

The identity of the reviewing IRB/PB, and the date of the approval of their waiver or alteration of the individual authorization. 164.512 (I)(2)(ii)
It must state that the IRB/PB has determined that disclosure of PHI poses no more than a minimal risk to the individual's privacy based at a minimum on these facts:
164.512 (I)(2)(ii)(A)(1-3)

    - The researcher has developed an adequate plan to protect the identifiers from improper use and disclosure;
    - The researcher has provided the IRB/PB a proposal to destroy the PHI that they are seeking as soon as their research permits, unless there is a health or research justification for retaining the PHI, or if another relevant law requires that the PHI be retained.
    - The researcher has provided written assurance that the PHI will not be disclosed to any other person or entity, except as the law requires for oversight, or for other research as permitted by the regulation.
  - It must state that the research could not take place without the waiver or the alteration of the individual authorization.
  - It must state that the research could not take place without access, and permission to use the PHI.
- A description of the PHI that is needed by the researcher, as approved by the IRB/PB.
- A statement that a waiver or an alteration of the individual authorization has been approved by either normal or expedited procedures of the IRB/PB.
- The documentation of the waiver or the alteration must be signed by the designated chairperson, or another board member designated by that chairperson.

Using Abstracted Data from Medical Records

HIPAA Case Study #1
Prepared by Don Steinwachs

Background: A longitudinal study is undertaken by academic researchers to assess the impact of changes in organization and financing of mental health and medical care on persons with severe mental illnesses enrolled in a state's Medicaid program. The study is supported by a National Institutes of Health (NIH) grant.

Research Question: Introduction of Medicaid managed care is expected to reduce inpatient utilization with improved access through a telephone system and an expanded scope of services through changes in coverage and payment. The study will seek to assess the impact of changes on the quality of mental health care, patient-reported outcomes, and Medicaid costs among disabled persons with severe and persistent mental illness.

Research Design: The study will identify all Medicaid eligibles with a claims-based diagnosis of a severe mental illness (e.g., schizophrenia, major depression) who meet continuous Medicaid enrollment criteria. The claims and enrollment data are provided to the research team after removing any data items not needed for the study and after replacing Medicaid identifiers, names, and addresses with a study identifier. From this group, a representative sample of persons will be drawn, re-identified, and approached for in-person interviews, asking for informed consent and individual authorization for the interview and individual authorization to use their Medicaid claims and to abstract their medical records. A research data set is to be created for all eligible for the study, using Medicaid enrollment and claims data over multiple years. For the representative sample, Medicaid enrollment and medical and mental health claims are linked to in-person interviews at three points in time plus an abstract of medical and psychiatric chart data. The data set on the sample will be used to more precisely measure treatment and outcome variables. Cooperation is sought from the state Medicaid Administration to do this study. State and university Institutional Review Boards/Privacy Boards (IRBs/PBs) review the protocol. The university IRB has legal responsibility for the research and the state IRB seeks to further assure that the study meets the state's requirements to protect human subjects.

1. University researchers want to have access to Medicaid enrollment and claims data to identify the subset of the universe of Medicaid enrollees who meet diagnostic, utilization, disability, and enrollment criteria. Since these criteria [to distinguish them from "continuous enrollment criteria"] could be applied in different ways and yield somewhat different populations, the investigators want access to inpatient and ambulatory claims for all Medicaid enrollees with continuous enrollment over a two-year period. The investigators will obtain the data from the state Medicaid agency.

> **Q:** Will the Common Rule apply to this research project, and if so, how?
> **A:** The Common Rule will apply to this study because it is supported by an NIH grant. The research would not fall under Common Rule exemption category 4 (45

C.F.R. § 46.101(b)(4)) because some new data will be collected. Many IRBs would not consider the research to fall under exemption category 2 (45 C.F.R. § 46.101(b)(2)) because sensitive data may be linked with identifying information. The research would only fall under exemption category 5 (45 C.F.R. § 46.101(b)(5)) if it were conducted by or subject to the approval of HHS or CMS, and if it were deemed to be designed to study, evaluate, or otherwise examine the Medicaid program. If the state and university IRBs determined that the study was not exempt, it would be subject to the Common Rule. The IRBs may review the research using an expedited review procedure if they determine that the study presents no more than minimal risk to human subjects, although an expedited review procedure may not be used where identification of the subjects or their responses could be stigmatizing to the subjects, unless reasonable and appropriate protections will be implemented so that risks related to invasion of privacy and breach of confidentiality are no greater than minimal. Informed consent may be waived with respect some subjects, particularly for those who will not be approached for in-person interviews.

Q: Is the agency a covered entity?

A: Yes, in this instance the state by acting as an insurer is a health plan that is covered by the Privacy Rule.

Q: Can the agency provide the data as a public health entity?

A: No, because the agency is a covered entity.

Q: What if the project were conducted by state Medicaid researchers?

A: An individual authorization or an IRB waiver is still needed to obtain the data under HIPAA. If more limited data were needed, a limited data set could be obtained with a data use agreement.

If the study is conducted by or on behalf of the state Medicaid agency as part of a quality assessment initiative and not primarily to obtain generalizable knowledge, then the project could potentially be considered "health care operations" under the Privacy Rule instead of research, and an authorization or waiver of authorization would not be needed; however, this characterization is unlikely if there is already IRB oversight of the project and informed consent will be obtained. One factor used to determine if an activity is designed to develop or contribute to generalizable knowledge is whether the results will be published or otherwise placed in the public domain. Because it may be more difficult to publish the results of the evaluation if IRB approval is not secured at the outset of the activity, a researcher should apply to an IRB for approval (and for consent and authorization waivers, if appropriate) if he or she may at some point wish to publish the results.

Q: Are there different approaches to getting de-identified information and the limited data set?

A: Yes, the limited data set provides some identifying information and can only be released for research, public health, and other health care operations. To obtain a limited data set, researchers must sign a data use agreement with the covered entity. No such agreement is necessary for de-identified data since all identifying

information has been removed and is, therefore, no longer subject to the Privacy Rule.

Q: Are there any special concerns related to the investigators reviewing mental health data?

A: While the Common Rule does not raise special concerns, the researcher will need to consider the potential stress of the patients being contacted based on a diagnosis such as schizophrenia. The IRBs will want to know what the surveyor will say when he or she contacts these subjects for an interview. The sensitivity of the data is also likely to influence the IRB's assessment of the study, including the privacy protections the IRBs will expect, the risks associated with the study, and whether the study can qualify for an exemption from the Common Rule or for expedited review. Moreover, the researcher will need to consider whether the potential subjects are competent to consent to participate in the study, or whether consent from a legally authorized representative must instead be obtained. Finally, state laws often create special protections for mental health information, and researchers may be required to take additional steps in order to access this information.

Q: Behavioral health information of individuals is being treated differently from other forms of protected health information; covered entities are not releasing it. What is the legal ruling behind this?

A: The only special protection for mental health information under the Privacy Rule is for psychotherapy notes. Psychotherapy notes are notes documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Under the Privacy Rule, an individual authorization is required to gain access to psychotherapy notes for research purposes for studies begun after April 14, 2003; neither obtaining an IRB waiver nor creating a limited data set is sufficient. State law may impose further restrictions on disclosure of mental health information for research purposes. Of course, covered entities (CEs) do not have to release protected health information (PHI) to researchers, but we hope they will continue to do so whenever allowed by state and federal law.

Q: Are dates in individually identifiable health information considered protected health information?

A: Yes, that is why they are removed. A limited data set may contain dates however, and as such would be preferable for research.

Q: In this scenario, is a limited data set a viable option?

A: No, a claim number is needed, and that is not a permissible variable within a limited data set.

Q: In soliciting for interviewees, which is preferable: an opt-out or an opt-in approach?

A: On first glance, it makes sense that more subjects will be available by having them return the card if they choose to opt out. IRBs are permitted to grant a waiver of consent and authorization under either approach, although some IRBs prefer opt-ins for subject recruitment to minimize coercion or unwanted contacts.

2. Investigators have identified the state Medicaid population with severe mental illness and continuous enrollment that they would like to have participate in this study from the data obtained from the state Medicaid agency and have drawn a representative sample to be approached for interviews. The investigators want the names, addresses, and other relevant information sent to the survey research firm which will be doing the interviewing.

Q: How will the information be developed to establish interview candidate information?
A: It may be best for initial contact of eligibles to come from the state Medicaid Agency, with the option to reply going directly to the survey firms. In this way, Medicaid does not know who responded, and the interviewees will not receive a cold call.
Q: In the past, IRBs permitted this protocol, having potential subjects send a reply card. Is this allowed under HIPAA?
A: HIPAA touches on this issue in another way. A waiver of authorization from an IRB/PB will be needed in order to get the potential interviewees' addresses in the first place. This waiver should identify the person and/or organization making the contact.
Q: How does the survey research firm relate to the state Medicaid agency? Does it need to be a business associate of the agency, or be part of the research team under subcontract to the researcher.
A: To contact the potential subjects and ask them to sign an authorization, the survey firm will be working with protected health information on behalf of the covered entity. The covered entity will therefore need to have either a business associate agreement with the survey research firm or receive an IRB/PB waiver of authorization so that the survey firm can access PHI to contact subjects. When applying for the waiver of authorization, the covered entity will have to spell out what activities the survey firm will be undertaking. The covered entity may disclose PHI for the research itself only with an authorization or waiver of authorization.
Q: Is an IRB waiver of authorization needed to obtain disclose the data to the survey research firm?
A: Yes, if the survey research firm will contact subjects, either a business associate agreement must be in place between the survey research firm and the covered entity, or the covered entity must obtain a waiver of authorization for study recruitment. The IRB will want to review the researcher's protocol on how the subjects will be contacted before granting a waiver of authorization.
Q: Since the researcher will obtain individual authorization for the interview and use of the data obtained from the interview, is it necessary to have the IRB review the process beyond the initial contact stage?
A: Unless the activity is considered by the IRBs to be exempt from the Common Rule, the IRB must have continued oversight of the study. This includes a continuing review of the study at least annually and ongoing contact with the IRB in the event of any proposed changes to the study or any unanticipated problems involving risks to subjects or others (*e.g.*, identifiable study files are lost or

accidentally disclosed). If the study is not exempt, the IRBs will ask for the entire protocol of the research before it has begun. They may grant a waiver of authorization with certain preconditions such as IRB reapproval of the waiver after one year, or periodic compliance checks by the IRB.

3. The informed consent procedure requires evidence that the person with mental illness can give consent (if not too symptomatic to understand what is being asked). If a person cannot be interviewed due to mental status, permission is asked to interview a proxy but this requires informed consent, too, as well as individual authorization to use PHI if for research. The result is few proxy interviews yielding a lower than desired overall response rate. Consent and individual authorization are also given at the time of the interview to link claims data and abstract of medical records to Medicaid claims. Interviewer training is required to avoid any suggestion that the desired respondent is mentally ill when efforts are made to locate for the interview. Also, training is given to assess the ability of a person to provide informed consent and to react appropriately if person is suicidal.

Q: Can the mentally ill give informed consent?
A: Yes, if they are considered legally competent. Researchers may need to evaluate a subject's capacity. A good policy may be to have a legally qualified mental health professional evaluate a subject's ability to give consent. IRBs will likely want some reassurance that the interviewer is well-trained for the task. In general, it is safe to proceed with a subject when they have been deemed competent both to participate and to consent to participation, have agreed to enroll, and have given consent.
Q: Can consent be obtained at the time of the interview?
A: In practice it may be a good idea to have a separate session with the subject on whether the subject is competent, and obtain consent at that time, then schedule a follow-up appointment to conduct the interview itself.
Q: Can an IRB approve a study without individual consent?
A: Yes, through a waiver of authorization and consent, but it may be more difficult to obtain such a waiver for a study of sensitive populations such as this one. IRBs grant authorization waivers on the grounds that: 1) it is impracticable to get an authorization, 2) there is minimum risk to individuals' privacy (not likely here), and 3) the study would be impossible to conduct without a waiver.
Q: If a person is upset after being contacted, does he or she have the right to sue?
A: Neither the Privacy Rule nor the HIPAA statute grants private parties the right to sue for alleged violations; individuals may only make a complaint to the government. If a waiver of authorization was granted by a relevant IRB and the waiver documentation meets the relevant requirements, the researcher would not likely be penalized for a Privacy Rule violation. Depending on how the person claims to have been wronged, the person may be able to sue under state law.

4. The investigators receive complete claims data, mental and medical, for the entire universe of eligible Medicaid enrollees (identity numbers scrambled) and for the sample,

whether or not, they consented. This allows investigators to test hypotheses on the universe and on the sample, using enrollment and utilization data to adjust for non-response bias. The Medicaid agency provides only the specific data items requested and approved by the IRB, not the complete enrollment and claims history files.

> **Q:** Are scrambled identifiers considered protected health information?
> **A:** The government interprets scrambled identifiers to be identifying information because they are derived from identifying information. Thus, a scrambled health plan beneficiary number is considered to be an identifier, even though the individual digits have been re-arranged. A truly random code, on the other hand, usually will not be considered an identifier; however, if the researcher has the key to the code in order to link the data back to the subject's identity, the researcher is considered to have PHI.
> **Q:** What happens to the records of those who decided not to participate in the study?
> **A.** When establishing protocols with an IRB, the researcher should let the IRB know what will happen to information collected on those who decide not to participate. Will the data be returned, destroyed, or kept to determine sample bias? The IRB will then have the opportunity to determine if the protocols are acceptable given the study.
> **Q:** Is it possible to obtain some data on those who do not want to participate to determine the type of bias in the sample?
> **A:** Protocols would have to be submitted to the IRB and a waiver of consent and authorization granted in order to receive any PHI. Non-response bias can be assessed by requesting the overall demographics of the eligibles from the survey firm, and comparing those with their own sample.
> **Q:** What happens if a waiver of authorization is granted and the covered entity still refuses to release the data?
> **A:** HIPAA states that a covered entity may rely upon the judgment of an IRB/PB, but that it is not required to do so. If a covered entity says no, then the researcher might want to talk to the covered entity's privacy officer directly, but otherwise there are few other avenues to pursue. If researchers are having trouble collecting data from covered entities, they should go to http://services.aamc.org/easurvey/survey/login.cfm to participate in the survey.
> **Q:** How long can the researcher keep data for things like publication, verification, or checking scientific validity?
> **A:** When the researcher applies for IRB approval and fills out the waiver request, it is important to specify how long the data will be needed (e.g. one year, until end of research project). It is also important to explain how the data will be protected until the time at which it can actually be returned or destroyed.

5. The investigators contracted with a firm to abstract records in the primary care and mental health specialty provider offices. The contractor received patient-identifying information from the Medicaid agency through a contract. The investigators received the abstracted information with the scrambled Medicaid number.

Q: What is the relationship between the abstracting firm and the researcher?
A: The contractor is the agent of the researcher. A health services researcher is usually not a covered entity in his or her own right, but if the researcher is employed by or a business association of a covered entity and the research is being conducted under the auspices of that covered entity, the researcher should check with that covered entity to determine whether the contractor should enter into a business associate agreement with the covered entity. For the contractor to obtain PHI directly from Medicaid or from HIPAA-covered primary care and mental health specialty provider offices, a waiver of authorization must be in place and must permit this activity, unless all subjects have signed authorizations allowing access. The IRB should be aware of any contractors and steps that will be taken to protect the data while under its control.
Q: Would this process need to be explained to the IRB before the researcher undertakes the project?
A: An IRB may want to see how the researcher will pass data to the contractor, and how the contractor will protect the data before it will grant a waiver of authorization. The waiver request will need to describe to whom the researcher, Medicaid, and the providers will release information.

6. In order to conduct the interview surveys, the state Medicaid agency formally contracts with a survey research firm to work as an agent of the state to undertake the survey and guarantee to safeguard confidentiality of patient-identifying data. Money to cover survey costs comes through separate contract with the university.

Q: What is the relationship between the state and the survey research firm? Between the firm and the researcher?
A: The firm may be considered a business associate of the Medicaid agency, but likely is not a business associate of the researcher. The Department of Health and Human Services has said that whether a business associate contract is required depends on the services, functions, or activities that a researcher is providing to, or performing for, the covered entity. Firms that conduct research 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). If the survey is considered research and not a quality assessment activity, then a business associate contract may not be required with the Medicaid agency as the researcher will not be performing services for the covered entity. Moreover, the university-based researcher likely is not covered by HIPAA in his or her capacity as a researcher; thus, no business associate agreement with the researcher or the university would be required, regardless of the services provided by the firm. However, a contract limited data use may be a good idea.
Q: Since the firm is acting as an agent of the state, does this process have to be approved by the IRB?
A. Yes. Unless the project is being conducted as “quality assessment” and will not be published, then it falls under the Common Rule and the research provisions of

the Privacy Rule and must go before an IRB in order for the covered entity to release any data.

Q: What if the protocol calls for data from dozens, or hundreds, of small practices?

A: Those small practices covered by the Privacy Rule may disclose PHI in reliance on subjects' authorizations or on a properly documented waiver of authorization, so long as the authorization or waiver contemplates disclosure of data by these small practices. The practices need not require the researchers to sign business associate agreements.

Linking Administrative Data to Chart Reviews

HIPAA Case Study No. 2
Prepared by Mitzi Dean and Hal Luft

Background: California law mandates hospitals to report data from routinely produced hospital discharge abstracts for the development of public reports comparing hospital outcomes for selected medical conditions for patients treated in California hospitals. As part of this mandate, the state agency responsible for the reports contracts with a California-based university to develop and validate a hospital-level risk adjustment model for community-acquired pneumonia (CAP). This validation study is designed to test whether it is worthwhile to produce and publish hospital-specific reports on outcomes of patients with CAP.

Research Design: A dataset comprised of information reported to the state about all patient discharges from eligible California acute care hospitals will be requested by the university researchers from the appropriate state agency. This patient-level dataset includes some of the 18 patient identifiers such as date of birth and exact admission and discharge dates defined by HIPAA as PHI and is, therefore, not a de-identified data set. Project staff will then extract information from this discharge data file for only those adult patients with a project-defined diagnosis of CAP. The patient characteristics or conditions reported as present at the time of admission of the CAP patients will then be used to develop a method for quantifying the risk of death within 30 days of CAP hospital admission. In the process of assessing the risk adjustment model, it will be necessary to estimate the potential for and to evaluate the impact of systematic error on the risk-adjustment model. This validation study will require asking a sample of 82 hospitals to submit, voluntarily, copies of 10 randomly selected patient charts. To make these chart requests requires that specific patient identifiers and admission dates be provided to the hospital. The hospital then will return copies of the patient charts by mail to the project director at the project headquarters at the university. Once the charts are received, a team of coding professionals, under contract to the project, will recode the ICD-9-CM principal and secondary diagnoses and procedures. Project Staff will then extract clinical information that is needed for the validation study from the same set of charts. The charts will then be destroyed.

While, in theory, hospitals could have abstracted the necessary information and passed on to the researchers only a file without identifiable information, this would have been so burdensome as to have reduced cooperation to nil. Furthermore, since a key part of the validation study was to determine whether abstracting by the hospitals resulted in systematic coding bias, relying on the hospitals to do the coding would have negated this part of the validation study.

1. This project was undertaken by the university under contract to the state agency.

Q: Will the Common Rule apply to this research project, and if so, how?

A: Whether the Common Rule or IRB review will apply to this activity depends on whether the activity is considered "research," as opposed to quality assessment, public health, oversight, or a related activity. Universities and hospitals often require that their IRBs or IRB staff make that determination, rather than the researchers themselves, if there is any chance that the activity could be considered "research." If the activity is considered "research" by these institutions, the Common Rule could apply even if the study is not funded by a federal grant. Institutions typically promise to the federal government, as a condition of receiving federal funding for any research, that they will apply the Common Rule to all of their research, even if that research would normally be exempted from the Common Rule. (This promise is made in a document called an "Assurance.") Given that no new data will be collected from subjects, the activity would be considered by the IRB to be exempt research (and the Common Rule would not require further IRB intervention) if the researchers only record information in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects. However, if project staff extracts identifying information from the records to provide to hospital staff or for other purposes, the project likely would not be exempt from the Common Rule. Even if the project is not exempt, it may qualify for expedited review by the IRB, and for a waiver of informed consent.

Q: Is the state acting as a covered entity?

A: If the state Medicaid program is acting as a health plan, such as via the Medicaid agency, it is a covered entity. If it is acting in its oversight capacity then it is not. In this instance, it is acting in its oversight capacity if it is not developing the risk adjustment model as part of a state health plan (e.g., Medicaid) quality improvement or pay-for-performance project.

Q: If the state were a covered entity and this study was undertaken as a quality assessment program, would it have to go through an IRB?

A: Perhaps. A covered entity may under certain circumstances disclose PHI for its own quality assessment purposes. However, given the state's role, this activity is not likely "quality assessment" as HIPAA uses that term in its definition of "health care operations." The state is not assessing the quality of its own services as a covered entity; rather, it is assessing the quality of the hospitals it licenses. Moreover, because the activity bears some indicia of research, some institutional policies may require that it be submitted to an IRB to determine whether it is subject to the Common Rule. A written determination by an IRB that the study is either exempt or approved would be helpful if the researchers or the agency wished to publish the findings in a scholarly journal.

Q: Can data collection count as a public health activity?

A: Hospitals can provide hospital discharge abstracts to the state if they are required by law to do so. Once the state receives the data, so long as it does not receive the data in its capacity as a covered entity, the Privacy Rule does not apply to the further use or redisclosure of the data by the state. If the state receives the data in its capacity as a covered entity (as determined by the state), then the state will need to: 1) determine whether the activity constitutes "research" under the Privacy Rule and the Common Rule (which use the same definitions of

"research") and, if so, 2) receive documentation of an IRB waiver of authorization (and perhaps informed consent) before disclosing or using identified data for the research. If the state receives the data in its capacity as a covered entity and concludes that the activity does not constitute research, it will need to determine under what other Privacy Rule exception (e.g., health care operations, or health oversight activities) it may disclose or use the data.

Q: If parts of the state are considered to be a covered entity, and other parts are not, is the part that is *not a covered entity* held to HIPAA Privacy Rule requirements?

A: No.

Q: What types of review are needed and by which bodies?

A. Assuming the project is "research" and if individual authorizations are not practicable (and they are not in this case), then a waiver of authorization is needed from an IRB or privacy board to meet the requirements of the HIPAA privacy rule. The university may have its own requirements for approval of any work undertaken by its employees. Likewise, the individual hospitals may require their own reviews, or they may in some cases decide to rely on the reviews of the state or university IRBs.

Q: Would these answers change if the project were initiated by the researchers and funded by a federal agency such as AHRQ, or a private group such as the California Healthcare Foundation?

A. In obtaining protected health information for research purposes from any covered entity regardless of source of funding, one of two things must happen to meet the privacy rule requirements. Researchers must either obtain individual authorizations to use the data from the subjects or they must obtain a waiver of authorization from an IRB or Privacy Board and present the required documentation to the covered entity. If the area of the state government receiving the data is not a covered entity under the public health or Privacy Rule exception, then the Privacy Rule does not apply to subsequent disclosures and uses of identifiable health information, unless the information is subsequently received by a covered entity. The receiving covered entity is then bound in its use and disclosures of the information, which has become protected health information again in its hands.

Q: What happens if neither your institution nor your state has an IRB?

A: There may be a state privacy board, even if the state does not have an IRB. In addition, any university or hospital that receives any federal funding for research either will have its own IRB or will have designated one or more external IRBs to review the institution's research. Another alternative that could be considered are commercial IRBs, but they can be quite costly. It is unlikely that physicians or other non-institutional providers will have an IRB.

2. The investigators need access to the identifiable Hospital Discharge Data (non-public format) in order to later request specific patient charts from reporting hospitals. (A public format converts the date of birth to age, the admission date to the day of the week, etc., and cannot be used to identify a specific patient chart). To assist the hospitals in locating the charts (because the state agency does not have medical record numbers), exact dates

of admission and discharge, patient birth dates, and social security numbers are needed. Social Security numbers are available in the non-public data.

Q: Does the non-public version of the data needed for this project meet the criteria of a limited data set?
A: No. The Social Security number is needed, and it cannot be included in the limited data set. Since protected health information must be used, the researcher must go through the IRB/PB process to obtain the data from the state, if the state holds the data in its capacity as a covered entity.
Q: What are the advantages to the researcher if a limited data set could be used?
A: The information can be released through a data use agreement, avoiding individual authorizations and/or IRB waivers and accounting for the disclosure of their protected health information. However, if the data disclosures to the researchers are "required by law," the protected health information needed to comply with the law may be released, with covered entity permission, without the covered entity's parsing the data further or negotiating a data use agreement.
Q: What would be needed to obtain approval from the relevant IRB(s) to obtain a limited data set?
A. Under the privacy rule IRB review is not required to approve access to the limited data set. The only approval necessary is the valid data use agreement signed between the researcher and the covered entity. There may be separate obligations to obtain IRB approval under the Common Rule, as described above.
Q: If covered entities are not required to release data, are there actions researchers can take to increase the response rate?
A: While there is no way to compel the release of data for this project absent a law requiring disclosure, researchers can help increase the response rate by understanding the Privacy Rule themselves. That way, they can initiate discussions with relevant personnel at the state (when obtaining data from the state) and at the hospitals about the relevant legal requirements. Having discussions with hospital chains before initiating the approval process, or working with their associations (American Hospital Association, Catholic Hospital Association, etc.), is also helpful. Data use agreements are another way of making a covered entity more comfortable with the proposal. Another idea is to include something in the study that would be useful to the hospital.
Q: What if I have an individual authorization and hospitals still refuse to send records citing HIPAA as their rationale?
A: Under the Privacy Rule, patients have a right to receive a copy of their protected health information. Patients can request the record and then forward it on to you. Note that the risk of accidental disclosure is higher in this instance. If researchers are having trouble collecting data from covered entities they should go to http://services.aamc.org/easurvey/survey/login.cfm to make their advocates aware of any problems.
Q: Can the state compel the hospitals to release data?
A: This depends on its specific state law. If there is a law mandating disclosure, then yes.

Q: During research preparation, when a researcher may have legitimate access to records in order to determine the protocols of the investigation under the Privacy Rule, can the researcher copy the records, black out identifiers, and then come back for the copied charts with the protected health information removed?
A: It is unlikely that a regulator would allow a researcher to do this when they are supposed to be reviewing records to determine if there is enough information available to warrant a study. One valid approach would be to sign a business associate agreement with the covered entity, remove the identifiers as part of the covered entity's health operations and then come back as a researcher and request the information.
Q: What if the researcher were able to obtain individual authorizations?
A: With individual authorizations, the Privacy Rule does not require IRB/PB review. Other aspects of the study may need IRB review, depending on the researcher's and data sources' institutional policies with regard to human subject protection and applicability of the Common Rule.

3. The investigators need data extracted from the clinical chart in order to validate the diagnoses and other clinical characteristics used in the risk adjustment model. Hospitals copied the requested charts and sent them to project headquarters. To assess the coding bias issues, the project does not require sensitive PHI to the analysis, but information such as the names and addresses is likely to be on each page in the medical record.

Q: Does obtaining a copy of the full record violate the "minimum necessary" provision of HIPAA?
A: It may. It is up to the IRB/PB to determine whether the protocol, which contemplates disclosure of the full record, meets the authorization waiver criteria set forth in the Privacy Rule. One criterion that must be met is that research could not practicably be conducted without access to and use of the PHI for which a waiver is requested. If a researcher can convince the IRB/PB that the entire record is needed, or it is impractical to request that the hospital remove all the non-necessary PHI from each page, and the IRB/PB grants a waiver of authorization stating that the entire record may be utilized, then the covered entity is specifically permitted by the Privacy Rule to rely on an appropriately-documented waiver in making its minimum necessary determination.
Q: Does this mean that the unnecessary information needs to be blacked out?
A: While this is up to the individual IRB/PB, the IRB/PB might tell the researcher that it does not believe it is unduly burdensome for the hospital to remove the unnecessary information.
Q: If the project is to obtain copies of the charts, who are the covered entities?
A: The covered entities are the hospitals that have the charts.
Q: Which IRBs have to approve the protocol?
A: While under the Privacy Rule only one IRB needs to approve the protocol to grant a waiver of authorization, many covered entities will not accept a waiver of authorization from every IRB; instead, some covered entities will accept waivers only from certain IRBs (or only from their own affiliated IRBs). The covered entities may also require that their own IRBs review the project for Common Rule

purposes. Depending on how many want to perform their own reviews, in this instance, the researcher may have to go through as few as one IRB/PB or as many as 83 (82 hospitals plus the university's IRB).

Q: If the university IRB approves, must the IRB/PBs of all 82 hospitals agree to accept that approval as binding? But ,if this is not a requirement of the 82 hospitals and the hospitals agree nonetheless to provide their records, what should they do to be compliant under HIPAA ?

A: Under the Privacy Rule, the hospitals may accept the university IRB's waiver of authorization (if the form of waiver complies with applicable requirements) and release the information accordingly. However, they are not required by the regulation to accept the waiver. If it wishes, the hospital can require the researcher to go through its own internal IRB before releasing any information. Hospitals typically have policies and procedures that address which external IRBs can grant waivers on which the hospital will rely.

Under guidance issued by the Office for Human Research Protections (OHRP), an institution is typically considered "engaged in research" if it releases individually identifiable private information for research purposes without subjects' explicit written permissions. So, the hospitals will also be bound by the terms of their Assurances with respect to their abilities to rely on an external IRB's review of the research under the Common Rule.

Q: Besides being liable for improperly releasing data, what other issues are facing covered entities?

A: Covered entities must maintain a detailed record of all disclosures of information made pursuant to an IRB waiver. While there are simplified procedures for maintaining these records when the disclosure involves 50 or more individuals, this so-called "accounting" requirement can be burdensome for covered entities.

5. Suppose project staff received authorization from each individual to request charts from the appropriate state agency and from the administrator of each affected hospital. Participation was voluntary. The request for specific patient charts was done through registered mail. Chart copies were received through registered mail. Charts were stored in locked cabinets inside a research suite that was locked at night. All charts were destroyed at the end of the project and an affidavit affirmed their destruction.

Q: Would anything need to be different in this process under the HIPAA Privacy Rule?

A: Probably not. The Privacy Rule requires only that covered entities have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The Security Rule, with which covered entities (except small health plans) must comply as of April 20, 2005, contains more detailed standards, but it applies only to electronic PHI.

6. The risk adjustment system cannot be validated effectively from administrative data alone. It is necessary to check the coding of each risk factor. The highly skilled

professionals needed for recoding of ICD-9-CM codes would need to be supervised by the research team in order to assure consistency. Clinical abstractors were hired as part of the project staff. Contractors agreed in writing to meet all confidentiality standards. In addition, contractors were given in-service training that included the university's confidentiality requirements.

> **Q:** Post HIPAA, would this be allowed? If so, what would be the required safeguards? If not, how would you suggest the research objective be accomplished?
> **A:** The Privacy Rule should allow this, provided that the IRB has reviewed the protocols for how the coders were to receive the data and how they would handle it. Note that the Privacy Rule does not directly govern the relationship between the researchers and the contractors because the researchers presumably are not in the university's "health care component" and thus are not covered by HIPAA.
> **Q:** Does it matter if the abstractors are employees of the university, independent contractors, or working for another firm?
> **A:** It should not matter as long as an IRB/PB has had a chance to review the data handling protocols, which are relevant to its decision to grant a waiver.

7. Suppose that the project was undertaken as a service to the state in compliance with state law, rather than with the intent of publishing findings. Once completed, however, it is decided that the results warrant publication.

> **Q:** Would any of the decisions made previously be modified if the intent is to publish, or would the ability to publish be affected by any of the decisions that might have been made if the original intent was not to publish?
> **A:** Assuming that the university researchers obtained the data needed for the project in a legitimate way, the Privacy Rule will not affect their desire to publish the results of the study. Instead, their ability to publish will be governed by university policy and by the willingness of journals to accept for publication the results of a project initiated without IRB review. If the intent to publish or otherwise to develop or contribute to generalizable knowledge (e.g., to add to the knowledge base of the field, or to develop outcomes or principles with predictive value) was genuinely absent at the outset of the project, but later arises, the researchers should promptly notify the appropriate university IRB. While IRBs do not have the power retrospectively to approve past data collection and analysis, some IRBs will approve or exempt a proposal to use the data going forward as analysis of existing (i.e., already collected) data, and some IRBs might provide a letter to that effect. It is important that the researchers be upfront and honest with the IRB and other officials at the university, as an IRB's willingness to take this approach will depend on whether it believes that research intent truly developed after the project was underway, or whether it instead believes that the researchers conducted "research" without IRB oversight.

Ethnographic Research in a Medical Setting

HIPAA Case Study #3
Prepared by Daniel Dohan and Hal Luft

Summary: An ethnographic study is undertaken by a university-based researcher to examine how a public hospital emergency department (ED) manages the provision of care to indigent patients in everyday life.

Background: Hospital EDs are required by law to assess all patients who present at their doors, and to provide treatment to those patients determined to have an emergency medical condition. Previous studies show that this obligation can create problems for hospital EDs due to: a) *social use*: patients who present to the ED may be suffering from social rather than purely medical problems, and b) *tenuous financing*: patients who present to the ED may be poor and uninsured and thus unable to pay for services provided per legal mandate. While the problems of social use and tenuous financing are well documented, how ED care-providers actually manage them in everyday life is not well understood. This study seeks to examine these problems as they occur in the ED and to document how ED providers interpret and manage them in everyday life.

Research Design: This study will involve an ethnographic case study of a public hospital ED where the problems of social use and tenuous financing are known to be acute. Interactions between and among patients and providers in all areas of the ED will be observed by a trained ethnographer during all ED shifts and days. Field notes will be recorded *in situ* to document how the problems of social use and tenuous financing manifest themselves and are managed in everyday life. In-depth interviews will be conducted with providers in order to elicit their understandings of the problems of social use and tenuous financing and how they perceive they are managed in the hospital ED.

1. To conduct this ethnographic project, investigators need to have full access to all areas of the ED while disturbing usual work routines as little as possible. This makes it difficult, if not impossible, to obtain signed consent forms from subjects involved in ethnographic research. In the past, some universities had taken the position that if this research was not federally funded, an IRB review was not required.

> **Q:** Will the Common Rule apply to this research project, and if so, how?
> **A:** If the hospital receives federal funding for any research and has signed an Assurance with the government, the outcome should not depend on whether this particular study is federally funded. However, if the hospital has not signed an Assurance, and the study itself is not federally funded, it may be exempt from IRB review on that basis, subject to institutional policy. The Common Rule also generally exempts research involving the use of survey procedures, interview procedures, or observation of public behavior, unless the research data generated are potentially identifiable and sensitive. However, as mentioned above, many institutions that receive any federal research funds require that their IRBs or IRB

staff make this determination. If the research is not exempt on either basis, it may qualify for expedited review and a waiver of informed consent.
Q: Has HIPAA changed this result?
A: Under the Privacy Rule, a hospital technically "discloses" PHI to any person who sees hospital members treat patients. In the ED setting, these disclosures will occur many times, because EDs are crowded and busy. For these and similar situations, the Privacy Rule contains a category of permissible disclosures called "incidental disclosures;" one example the government has given of a permissible incidental disclosure is when a hospital visitor overhears a provider's conversation with another provider or a patient. However, incidental disclosures are only permissible if they are consistent with the hospital's minimum necessary policies and safeguard procedures. It is unlikely that a hospital could, consistent with these policies and procedures, knowingly allow researchers to observe its patients being treated without patient authorization or an IRB waiver. This is therefore an example of research that might be exempt under the Common Rule, but for which the Privacy Rule likely contains no exemption.
Q: What are the implications of HIPAA with respect to "authorization", and are these implications dependent on the source of funding?
A: The application of HIPAA does not depend on funding source. The study will likely require either patient authorization or a waiver thereof, as described above.
Q: Will IRBs be able to continue to grant waivers of authorization for ethnographic projects conducted in clinical settings?
A: Yes, but they will grant waivers based on the principle that the risk of patient identification is minimal. An IRB might waive signed consent, but require that the subject be informed verbally, in plain language.
Q: What is the covered entity in this case and how does it enter into the process if it is not directly providing data?
A: Even though the covered entity is not giving the researcher access to medical records, their granting permission to make observations in the Emergency Department is, according to the rule, granting access to protected health information.
Q: Would authorization and IRB approval be required if the researcher were to undertake the study standing outside the ED, observing people as they entered and left?
A: The answer is unclear. Assuming the hospital controls the premises outside the ED, the hospital controls whether the researchers have access to information they obtain and may thus be viewed as "disclosing" this information. However, the amount of health information in these disclosures is significantly reduced or even eliminated, to the extent it is not plainly obvious that someone entering or leaving the ED will be or had been a patient at the hospital.
Q: Does individual consent need to be gathered if the subject is a doctor?
A: As long as the subject is not a patient, and the researcher does not obtain from the subject any individually identifiable health information about a patient, then the Privacy Rule does not apply to the researcher's interaction with the doctor. Whether consent to participate in the study (i.e., Common Rule informed consent) must be obtained from the doctor is up to the IRB.

Q: Can the IRB determine that the investigator cannot record certain identifiable information in the field notes? How should the investigator raise this issue with the IRB?
A: By the law of "small numbers" an IRB may determine that a researcher cannot record certain information on the basis that is identifies a certain person, (e.g., a description of the subject's behavior or appearance). A solution is to de-link the times and dates of observations with the interview portion of the investigation. Note that recording identifiable information, particularly if the IRB believes that some of the notes may be sensitive (e.g., about a patient treated for a drug overdose, suicide attempt, sexually transmitted disease, etc.), may jeopardize the study's exemption under the Common Rule.
Q: How should the investigator raise this issue with the IRB?
A: The researcher needs to outline the protocols that will be involved, how the observation will take place, how decisions will be made to determine who to interview, the approach, what type of oral consent the researcher plans to obtain, and what will be recorded in the notes.

2. While conducting ethnographic research in the ED, researchers will invite some patients to participate in the study and their oral authorization (and consent) will be obtained.

Q: Are oral authorizations allowed under HIPAA?
A: Oral authorization may be allowed by the IRB in the form of a waiver of *signed* consent if there is a sound reason why the research could not be conducted otherwise, and if it poses minimal risk to the patient. An example of when oral authorization may be permitted would be for telephone interviews.
Q: Can consent be gathered after the interview or observation?
A: Having the subject sign an individual authorization after the fact is permitted as a means of allowing any use or disclosure of PHI by a covered entity once the authorization is signed. There must then be some independent basis (e.g., waiver of authorization) under HIPAA that allowed the hospital to grant the researcher access to patients before the authorization was signed.

3. Investigators will inevitably be exposed to identifiable information related to other patients who are not participating in the research, for example, when providers discuss the medical condition of a non-subject patient in the presence of the investigator.

Q: How could this "collateral" information be used in research?
A: It is important to address how this will be handled with the IRB. In addition, if the researchers are not collecting this collateral information for research purposes and their exposure to this information is not intentional, then the disclosures might constitute permissible "incidental disclosures," as described above.
Q: Does the IRB need to approve this protocol under the Privacy Rule?
A: If a waiver is sought for the researchers to collect these data, then IRB review would be required. The IRB would consider, among other things, the researcher's plan for protecting sensitive information. It is also a good idea to check with the

IRB periodically (or as directed by the IRB) to maintain assurance that the agreed-upon protocols are being followed.

4. To record ethnographic data confidentially, investigators generally use a code system to record individual identities in field notes and use pseudonyms and disguise identifiable characteristics of participants or settings in publicly available research reports. Investigators and other key members of the research team maintain access to the original field notes containing all identifying information (except actual names). Access to raw data is restricted, field notes and interview data are kept in locked filing cabinets and password-protected computer files.

Q: Will these practices for maintaining subject confidentiality change because of HIPAA?
A: Probably not. The Privacy Rule requires only that covered entities have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The Security Rule, with which covered entities (except small health plans) must comply as of April 20, 2005, contains more detailed standards, but it applies only to electronic PHI. If researchers are interested in protecting the notes from legal process (such as a subpoena), they should consider seeking a Certificate of Confidentiality for their research from the National Institutes of Health, as a court could compel disclosure not only of the coded notes, but also of the linking information needed to identify the notes.
Q: What must the researchers disclose to the covered entity about how they will store and use the data?
A: Some of these details may be included in the waiver of authorization document supplied by the IRB to the covered entity. Even though the researcher is not required by HIPAA to supply additional information, hospital policies may require that other hospital personnel (i.e., individuals not on the IRB) receive the protocol or a summary of it.
Q: Do protocols for storage and maintenance need to be approved by the IRB?
A: Yes, if the study is subject to the Common Rule or if a HIPAA authorization waiver is sought.

5. During interviews, investigators tell providers that they, the investigators, are not interested in the details of any particular case, but they also encourage providers to speak freely about their experiences of providing care in the ED.

Q: Will the practice of using one's own discretion in discussing patient information be sufficient under the new Rule? If not, what standards will apply?
A: No. The standards laid out in the HIPAA privacy regulation apply and will be used by the IRB to examine all privacy protocols and provide oversight of the study.
Q: Who/what will determine these standards?
A: The IRB will determine the standards using the criteria laid out in the privacy regulation.

Q: How will it be determined if the standards are violated?
A: The IRB maintains oversight over the research project, and the hospital or (in some cases) the IRB may stop the research if the approved protocol is not followed. In addition, patients are given the ability to direct complaints to the Office of Civil Rights. While the researchers in this case likely are not directly covered by the privacy rule, one can assume that if covered entities receive complaints about providing information to certain investigators that covered entities will no longer release data to them.
Q: What will the researcher need to disclose to the relevant IRBs in order to have his or her interactions with providers approved?
A: Researchers will need to disclose information regarding the protocols used to gather, protect, and store identifiable health information.

Collaboration among Multiple Hospitals

HIPAA Case Study #4
Prepared by Don Steinwachs

Research Design: A cross-sectional research study is undertaken by a researcher based in a private research center, funded through a grant from the federal government to compare treatment and outcomes for trauma patients between hospitals designated as trauma centers and community hospitals providing emergency medical services.

Research Question: The establishment of regionalized systems for trauma care, including the designation of trauma hospitals to treat the most severe cases, varies widely across states and regions. Regionalized systems are expected to triage patients based on severity and transport the severely injured to specialized trauma centers. The research study seeks to evaluate the relative effectiveness of designated trauma centers in achieving improved patient outcomes, including increased survival and recovery.

Research Design: The study will use statewide hospital discharge abstract data to describe the distribution and severity of hospitalized trauma cases and in-hospital mortality. For selected categories (e.g., lower extremity, head trauma), samples of cases will be drawn, stratified by hospital and type and severity of trauma. The sampled cases will have their medical records abstracted and a follow-up questionnaire will be sent to patients approximately one year following the injury to assess outcomes. Quality of care indicators will be compared between designated trauma center and community hospitals, as well as outcomes among survivors. Cooperation is sought from the state emergency medical services authority, sampled hospitals, and from trauma survivors. The university IRB reviews the protocol, as does the state agency which provides access to hospital discharge data, and so do IRBs in most of the hospitals.

1. Investigators want to have access to all hospital discharge data in a state or region with hospital identifiers and case numbers. The data are used to compare trauma case mix and estimate inpatient mortality by type and severity of trauma, comparing hospitals with designated trauma centers and community hospitals. The data are then used to sample cases, stratified by hospital, injury and severity, for medical record abstracting and one-year follow-up to assess outcomes.

> **Q:** Would state agency reviews of the protocol and approval of access to hospital discharge data with patient demographic information, dates of admission and discharge, diagnoses and procedures, unique case identifier that the hospital can use to match to a patient, and hospital identifier be allowed by the Privacy Rule? Under what conditions? If so, what would be the required safeguards?
> **A:** Unless otherwise required by law, individually identifiable health information can only be released by hospitals for research purposes with an individual authorization or IRB waiver of individual authorization. If the researchers want to access data from the state, it is also important to assess whether the data holder is a covered component of the state. If a waiver is sought, the researcher will have to

convince an IRB or Privacy Board that the use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, the research could not practicably be conducted without the waiver or alteration, and the research could not practicably be conducted without access to and use of the protected health information.

Q: If not allowed by the Privacy Rule, how would you suggest the research objective be accomplished?

A: If an IRB waiver cannot be obtained, the researchers should consider to what extent a limited data set or de-identified data can be used.

Q: What kinds of data can researcher pursue?

A: Researchers can access any information that an IRB approves access to (pursuant to a waiver of HIPAA authorization and as required by the Common Rule and the institution's Assurance), and a covered entity agrees to provide. In this particular instance, the researcher is pursuing: 1) discharge databases (also includes quality of care indicators), 2) in-hospital mortality records, 3) medical records of sample patients that the researcher is requesting for the purpose of sending out questionnaires, and 4) patients' responses to questionnaires.

Q: Where do the hospitals as covered entities come into play in this interaction?

A: As covered entities, hospitals are liable for any misuse of protected health information. Hospitals are not required to release information for research purposes, even if an IRB has approved a waiver of authorization. The only times a hospital is required by the Privacy Rule to release information are: 1) if a patient asks for the information, pursuant to HIPAA's access provisions (an individual authorization is not required), and 2) when required by the Secretary of Health and Human Services to investigate or determine the covered entity's compliance with the Privacy Rule, and 3) pursuant to a state law requiring disclosure, usually to a state authority. This is permitted as an exception to the Privacy Rule, but is not required by the Privacy Rule.

2. Investigators have identified the study hospitals and a sample of trauma cases for medical record review and follow-up. They want the hospitals to provide names, addresses and other relevant information to a survey research firm which will be doing the follow-up interviews. Also, the investigators want access to the medical records to collect detailed information on the injuries and the treatments provided.

Q: Would hospitals be less likely to agree to participate in this study now that the Privacy Rule is in effect? Less likely than before? If so, what could be done to increase participation?

A: Some hospitals may be slightly more cautious about participating in medical records research in light of HIPAA, but there are a number of approaches a researcher can take in order to increase participation by covered entities. One is to form cooperative relationships with clinicians within the institution. Another is to consult directly with the privacy officer of the hospital regarding how the research protocols should be designed to meet their needs. Using an IRB the hospital has worked with before and trusts (if not a hospital-affiliated IRB) will also help.

Q: What risks do hospitals assume in permitting access to this information?

A: Hospitals are potentially liable under the regulation for improperly releasing protected health information. However, if they release information based upon an appropriately documented IRB waiver of authorization then the release should not be considered improper under the Privacy Rule by the government. However, bad publicity with patients and the surrounding community could result if the researcher misuses or inappropriately releases protected health information, and hospitals are vulnerable to lawsuits under state law. Hospitals also need to provide a record regarding the release of protected health information to any patient who asks. Tracking disclosures of this information as required by the Privacy Rule places quite a burden on the hospital (and all covered entities). It is important to address these concerns when designing research protocol, as well as when weighing the potential good versus the harm or burden that can occur through the investigation.

Q: Who within a covered entity usually de-identifies data or removes certain unnecessary fields from medical records?

A: In-house medical records staff could perform this function, or it could be performed by a contractor that has signed a business associate agreement with the covered entity.

Q: Under what conditions would the Privacy Rule permit the hospitals to disclose the protected health information to the survey research firm and to the researcher?

A: Hospitals are permitted to release protected health information if they receive proof of an individual authorization, if an IRB approves a waiver of authorization, via a limited data set with a data use agreement, or if it is data only about deceased subjects. This does not mean that the hospital will release the information. It is at their discretion as a covered entity whether to do so.

3. The hospital is asked to provide consent to access all sampled medical records for abstracting, including records for persons who died in the hospital and records for those who were discharged alive. This information will be used to make a final determination about eligibility for interview and will be linked to the discharge abstract data. Also, the hospital is asked to provide contact information for all those who were discharged and are eligible for a one-year follow-up interview to assess outcomes.

Q: Would the hospital be allowed to contact discharged patients for an interview without patient consent or individual authorization? Under what conditions?

A: Under the Privacy Rule, a hospital can contact a patient for these purposes only with previous individual authorization to do so, pursuant to an IRB waiver of HIPAA authorization, or if the contact is simply to ask the patient if he or she would be willing to sign an authorization to participate in the study.

Q: How is authorization acquired for decedent's information?

A: Either a waiver of authorization from a relevant IRB, or direct proof of the person's death, such as a death certificate, or an obituary, whatever the covered entity will accept. The covered entity might not request any proof of death, but the researcher needs to present it if asked by the hospital.

Q: Is passive consent permissible (e.g., assuming authorization if no response to a letter)?

A: This is permitted only by a waiver of authorization from an IRB. **Q:** Is it permissible to send the survey along with an individual authorization for use of the individual's protected health information?
A: Yes, so long as no covered entity has already used or disclosed PHI for research purposes, unless pursuant to an IRB waiver of authorization. Note that if the individual's survey response is sent directly to a non-covered entity researcher or non-covered research firm, and the responses do not pass through a covered entity, HIPAA will not apply to the survey responses.
Q: Can the authorization be in the form of a signature at the bottom of the survey?
A: Only if the IRB permits an alteration to the individual authorization. This is more likely to be permitted if the perceived risk is minimal.

4. The investigators link complete hospital discharge data with medical record abstracts to interviews from those who could be located and agree to be interviewed. This allows investigators to test hypotheses on the universe of trauma cases and on the sample, and to use the discharge abstract data to adjust for non-response bias where people could not be interviewed or refused consent.

Q: Under the Privacy Rule, could investigators be granted access to detailed, though de-identified medical information on all cases sampled, regardless of consent? Under what conditions?
A: Yes, but only if the information is de-identified within the meaning of HIPAA (i.e., all the specified identifiers are removed). De-identified health information is not protected by HIPAA.
Q: If so, what would be the required safeguards?
A: None, if the information meets the definition of "de-identified" under the regulation, then that information is not protected by the regulation. However, since de-identified information is less useful for research, a limited data set might be used instead. The limited data set requires a higher level of protection than de-identified information, including a requirement that the researcher and the covered entity enter into a data use agreement spelling out how the information is to be used and protected before the covered entity can provide it.
Q: If de-identified information is not sufficient, how would you suggest the research objective be accomplished? What strategies could be used to limit non-response bias?
A: Obtaining the contact information from the hospital, via an IRB waiver of authorization would allow the researcher to mail a letter to potential interview subjects asking them to return a postcard if they do not wish to participate in the research study. The IRB should also be asked to grant access to the medical records of those not participating in order to determine sample bias.
Q: What can the researcher do to convince hospitals to allow him or her access to patient contact information for the survey phase of the project?
A: Survey research firms can help to approach this question. Giving the hospital incentive to participate is always a good strategy. Another strategy is to ask clinical staff to get individual authorization on-site when the patient is there for treatment.

Q: What if the patient cannot sign an individual authorization due to the injuries received, and you will need to contact them many months after discharge?
A: The subjects may later be contacted either pursuant to an IRB waiver or by a business associate of the hospital (as part of the hospital's "health care operations") to ask the subject to sign an authorization. Or someone with the legal authority to act for the patient could sign an authorization for the patient.

HIPAA Privacy Resources

General

- *HHS Office for Civil Rights*
  Provides technical assistance materials such as copies of the rules and guidance documents, frequently asked questions (FAQs), and sample business associate contract provisions.
  http://hhs.gov/ocr/hipaa/assist.html

- *Privacy Regulation and Guidance/Office of Civil Rights*
  http://www.hhs.gov/ocr/hipaa

- *OCR website to submit privacy questions*
  http://www.hhs.gov/ocr/hipaa2.html

- *HHS, Office of the Assistant Secretary for Planning and Evaluation (ASPE)*
  Provides background information on Administrative Simplification Provisions and Rules including all versions of proposed and final rules, preamble to rules, and HHS's responses to comments on proposed rules. Useful when issue is not addressed in FAQs.
  http://aspe.hhs.gov/admnsimp/

- *Workgroup for Electronic Date Interchange (WEDI/SNIP)*
  Provides an excellent, publicly available resource materials developed by volunteers implementing all aspects of HIPAA for a wide variety of organizations. Contains excellent white papers describing the rules and implementation issues.
  http://snip.wedi.org/public/articles

- *American Health Information Management Association*
  Resource for medical records professionals, with detailed information on all aspects of handling and protecting medical records.
  http://www.ahima.org

- *American Health Information Management Association Practice Briefs*
  Oriented towards providers. Includes models and guidance for designated record sets, notice of privacy practices, minimum necessary, uses and disclosures, record destruction, consents, authorizations, marketing and fundraising, record retention, privacy official and security official job descriptions, and privacy training.
  http://library.ahima.org/xpedio/groups/public/documents/web_assets/bok1_016846.hcst

- *HIPAAGIVES*
  Provides a forum for those working for and with state and local government. Also maintains free HIPAA materials of all kinds developed by state and local government agencies. Must sign up and be able to demonstrate government connection.
  http://hipaagives.org/

- *International Association of Privacy Professionals*
  Privacy Officers Association web site with links to other HIPAA resources
  http://www.privacyassociation.org/index.html

Medicaid

- *Centers for Medicare and Medicaid Services (CMS)*
  The official site for HIPAA information related to Medicare and Medicaid. Includes a notice of privacy practices that has been reviewed for compliance.
  http://cms.gov/hipaa2/default.asp

Public Health

- The Privacy Rule and Public Health
  http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

Research

- The Privacy Rule and Research
  http://privacyruleandresearch.nih.gov/

Data Release (General)

- *National Center for Health Statistics*
  Data release policy
  http://www.cdc.gov/nchs/products/elec_prods/intro/relpolic.htm