Scripps Gerontology Center

Scripps Gerontology Center Publications

Miami University *Year* 2005

The HIPAA privacy rule and long-term care : a quick guide for researchers

Jane Straker* Patricia Faust†

*Miami University, commons@lib.muohio.edu

†Miami University, commons@lib.muohio.edu

SCRIPPS
GERONTOLOGY CENTER

396 Upham Hall
Miami University
Oxford, OH 45056
(513) 529-2914
scripps@muohio.edu
www.scripps.aging.org

The HIPAA Privacy Rule and Long-Term Care: A Quick Guide for Researchers

Jane K. Straker
and Patricia C. Faust

research organization, or the research sponsor nor may they be related to any individual who is part of these organizations; and members may not have conflicts of interest in regard to the projects that come under their review.

Protected Health Information (PHI): This is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or shared in any other form or medium. The 18 types of Protected Health Information (PHI) are: names, geographic subdivisions smaller than a state (street address, city, county, precinct, zip code (allowing the retention of the first three digits of zip codes if the zip code area contains more than 20,000 people), all date elements except the year (for example, admission date, birth date, or discharge date), all ages over 89 (allowing for ages to be collapsed into one category labeled "90 and over"), telephone numbers, fax numbers, e-mail addresses, Social Security numbers, medical record numbers, health plan numbers, account numbers, certificate or license numbers, vehicle identification/serial numbers/license plate numbers, device identification/serial numbers, URLs, internet protocol (IP) addresses, biometric identifiers (for example, fingerprints, voiceprints, and dental x-rays), full-face photographs and comparable images, and any other unique identifying number, characteristic, or code.

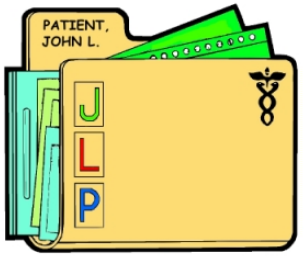
Separate Unit: A distinct entity housed within a larger organization. Sometimes a hospital is considered a separate entity within the larger university. In this case the hospital employees would be considered "covered entities" but the university researchers would not.

Waiver of Authorization: Written authorization from the Institutional Review Board (IRB) or Privacy Board that fully or partially waives the HIPAA requirement for individual participant authorization. Before a waiver is granted the IRB or Privacy Board must be satisfied that the participants' privacy and welfare will not be adversely affected by the researcher's use of protected health information.

※※※

The HIPAA Privacy Rule and Long-Term Care: A Quick Guide for Researchers

Jane K. Straker and Patricia C. Faust
Scripps Gerontology Center
Miami University, Oxford, Ohio
May 2005



Acknowledgments: Our appreciation goes to William Ciferri, Marshall Kapp, J.D., Roland Hornbostel, J.D., and Ian M. Nelson, M.G.S., for their comments on earlier versions of this brochure. Any errors remaining are the responsibility of the authors. Thanks to Valerie Wellin for her layout and editorial expertise.

This research was funded as part of a grant from the Ohio General Assembly, through the Ohio Board of Regents to the Ohio Long-Term Care Research Project. Reprints are available from Scripps Gerontology Center, Miami University, Oxford, OH 45056; scripps@muohio.edu; (513) 529-2914; FAX (513) 529-1476.

Downloadable:
http://www.scripps.muohio.edu/scripps/publications/HIPAA.html

Institutional Review Board (IRB): An IRB is a board or other group designated by an institution to review the legal and ethical aspects of research involving humans as subjects. The board is comprised of individuals from the organization, as well as outside representatives. Board members should have research expertise and an understanding of the issues involved in human subjects protections. IRBs have authority to approve of, disapprove of, or require modifications to all research activities covered by the federal human subjects rule (45 CFR 46). Hospitals, academic medical centers, government units, universities, and others engaged in research activities involving human subjects have their own designated IRBs or submit their protocols to an outside IRB for review.

Limited Data Set: The following identifiers must be removed from the health information if the data are to qualify as part of a limited data set: names; postal address information, other than city, state, and zip code; telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; health beneficiary numbers; account numbers; certification/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web universal resource locators (URLs); internet protocol (IP) address numbers; biometric identifiers, including fingerprints and voiceprints; and full-face photographic images and any comparable images. The limited data set can be used for purposes of research, public health, or health care operations without the researcher obtaining an individual's authorization for its use or disclosure as long as a data use agreement is in place.

Privacy Board: A privacy board is an alternative to an Institutional Review Board developed for the purpose of reviewing requests for alteration or waivers of research authorizations under the HIPAA statute. Privacy boards and the rules for their establishment were authorized by the HIPAA Privacy Rule. Members must have varying backgrounds and professional competencies; each board must have at least one member who is not affiliated with the covered entity, the

Data Use Agreement: The means by which covered entities obtain satisfactory assurance that the recipient of the limited data set will use or disclose PHI in the data set only for specified purposes. A written data use agreement meeting the Privacy Rule's (HIPAA) requirements must be in place between the covered entity and the limited data set recipient.

De-Identified Data: De-identified data are those with the following personally identifiable items removed: names, geographic subdivisions smaller than a state (street address, city, county, precinct, zip code (allowing the retention of the first three digits of zip codes if the zip code area contains more than 20,000 people), all date elements except the year (for example, admission date, birth date, or discharge date), all ages over 89 (allowing for ages to be collapsed into one category labeled "90 and over"), telephone numbers, fax numbers, e-mail addresses, Social Security numbers, medical record numbers, health plan numbers, account numbers, certificate or license numbers, vehicle identification/serial numbers/license plate numbers, device identification/serial numbers, URLs, internet protocol addresses, biometric identifiers (for example, fingerprints, voiceprints, and dental x-rays), full-face photographs and comparable images, and any other unique identifying number, characteristic, or code.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information.[2]

[2]Centers for Medicaid & Medicare Services. HIPAA Administrative Simplification Glossary. Retrieved March 9, 2005, from http://www.cms.hhs.gov/glossary/default.asp?Letter=ALL&Audience=7

Table of Contents

Glossary

Authorization Elements: Information that must be included in a written authorization of PHI. These elements are: a specific and meaningful description of the elements of PHI to be disclosed, the names or other specific identification about the person, persons, or class of persons (e.g. "researcher's staff") authorized to make the request for use or disclosure, the names or other specific identification of the persons to whom the covered entity may make the requested use or disclosure, a description of the purpose of the requested use or disclosure, an authorization expiration date or event (for research purposes "none" or "the end of the research project" are acceptable), signature of the individual or his/her legally authorized representative (with a description of the representative's authority, e.g. "John Smith, Power of Attorney for Jane Doe"), and the date. It also must include a statement that the participant has the right to revoke authorization at any time, an indication whether treatment or enrollment in services, or benefits is dependent on authorization, the consequences of refusing to sign the authorization, and a statement that the PHI may be re-disclosed by the recipient. (For example, a researcher might disclose PHI to a sponsor or funding agency. If the funding agency was a not a business associate of the research organization, nor a covered entity, the Privacy Rule would no longer apply although they would still be required to maintain confidentiality responsibilities under other laws.)

Business Associate: A person who performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information such as claims processing or data analysis. A person employed by a covered entity is not a business associate of that entity.

Covered Entity: A health plan, health care clearinghouse, or health care provider, and in some cases researchers, who use electronic transmission of health information in connection with a transaction in accordance with Health and Human Services' standards.

- Office of the Assistant Secretary for Planning and Evaluation U.S. Department of Health and Human Services
  http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm

- Office for Human Research Protections (OHRP), HHS
  http://www.hhs.gov/ohrp

- State of Ohio. HIPAA Ohio.
  http://www.hipaa.ohio.gov/

- Substance Abuse and Mental Health Services Administration (SAMHSA)
  http://www.hipaa.samhsa.gov/

- University of Minnesota
  http://www.irb.umn.edu/guidance/hipaa/faqhipaa.cfm#waiver

※※※

Introduction to HIPAA

The Health Insurance Portability and Accountability Act of 1996 (**HIPAA**)* was primarily designed to protect health insurance coverage for workers and their families upon a worker's change in or loss of employment. Besides insurance portability **HIPAA** has changed the way health care providers share and use **protected health information** (**PHI**) by establishing strict federal standards both for electronic data interchange (EDI) and for protecting patients' confidentiality.

The **HIPAA** Privacy Rule, effective in April 2003, is the first of three major changes that affect the entire health care delivery system as a result of Title II of **HIPAA**—Administrative Simplification. The second major change occurred in October 2003 when new rules governing the electronic exchange of data between providers and health plans went into effect. A final **HIPAA** provision regarding the security of data was effective in April 2005.

PHI includes 18 types of information such as patients' names, addresses, identification numbers—even their zip codes or license plate numbers. Health care consumers are notified of their rights to privacy every time they visit a new physician, dentist, or pharmacy. **HIPAA** was

Definition-Protected Health Information (PHI): This is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or shared in any other form or medium.

*Boldfaced terms are included in a glossary at the end of this document.

designed to protect the confidentiality of health care recipients and to prevent unauthorized access to and use of health care information. In addition to changes in the way our dentists, physicians, and pharmacists do business, **HIPAA** has also changed the relationship between long-term care service providers, their clients, and researchers. The scope of activity to which the **HIPAA** privacy rule applies is often viewed too narrowly. **HIPAA** applies to other types of providers and intermediaries besides doctors, hospitals, and health insurance carriers. Nursing homes and home care agencies are subject to **HIPAA** regulations as well. For example, the state of Ohio has determined that **HIPAA** applies to all its Medicaid home and community-based waiver programs such as PASSPORT.

Long-term care service providers often are approached by researchers for access to their clients or residents to participate in a variety of research studies. A group of gerontology students may want to interview residents about their lives during World War II, a faculty researcher may want to recruit caregivers for a study on time-use among families who receive home and community-based services, or a medical school researcher may want to test a gait-training program with older people prone to falls. Long-term care clients often provide a ready pool of participants who share some quality that is important to research.

Definition-
A **covered entity** is an organization that transmits health care information electronically for a variety of purposes such as payment. Although they may share health care information through a variety of other means – orally, or on paper, they are subject to **HIPAA** regulations.

Long-term care providers (**covered entities**) often invite researchers into their facilities or organizations to help them improve their services or to evaluate a new program or intervention.

Additional Resources

HIPAA Privacy Rule

- The final HIPAA Privacy Rule is available at http://www.hhs.gov/ocr/hipaa 45 Code of Federal Regulations, Part 160 and Subparts A and E of Part 164.

Agencies

- Office for Civil Rights (OCR), Department of Health and Human Services (HHS) http://www.hhs.gov/ocr/hipaa
- Agency for Healthcare Research and Quality (AHRQ) http://www.ahcpr.gov/
- Centers for Disease Control and Prevention (CDC) http://www.cdc.gov/nip/registry/hipaa7.htm
- Food and Drug Administration (FDA) http://www.fda.gov/
- Indian Health Services (IHS) http://www.ihs.gov/AdminMngrResources/HIPAA/index.cfm
- Mental Health in Ohio HIPAA Website http://www.mh.state.oh.us/hipaa/hipaa.index.html
- National Institutes of Health (NIH) http://privacyruleandresearch.nih.gov/
- North Carolina Healthcare Information and Communication Alliance, Inc. (NCHICA) http://nchica.org/

agreement, it has violated the Privacy Rule. If a **covered entity** knows a recipient with a **data use agreement** has violated the agreement the **covered entity** must take steps to correct the activity or practice. If these steps are not successful, the **covered entity** must discontinue disclosure of **PHI** to the recipient and notify the Department of Health and Human Services.

This summary provides a brief look at **HIPAA** and its implications for research in long-term care. The information in this brochure is designed to educate and promote discussion and should not be construed as legal advice. Final decisions as to the appropriate strategies to be followed for researchers should be made by **Institutional Review Boards** and, where necessary, with advice from appropriate legal counsel.

※※※

Long-term care providers may allow researchers to interview their residents as part of an evaluation of long-term care services, or they may allow gerontology students to interview residents as part of a research methods class.

The problem today is how to ensure that important research regarding long-term care service provision continues, while protecting long-term care providers and clients. The questions below are designed to address the **HIPAA** issues relevant to researchers in long-term care.

※※※

Who is affected by the HIPAA statute and implementing regulations?

Any health care plan, health care clearinghouse, or health care provider that transmits individually identifiable health care information electronically is a **covered entity** and is required to comply with **HIPAA**. A long-term care facility that transmits data to the state Medicaid office electronically is a **covered entity**. A service provider that submits claims to Medicaid is a **covered entity**. Researchers might also be considered **covered entities** if they are employed by a university that has a hospital — unless the hospital is designated as a **separate unit** within the university, and the researchers are not employed in that **separate unit**. In that case, only the hospital and its workforce would be **covered entities**. However, researchers who receive health care information from **covered entities** have certain obligations under **HIPAA**. **Covered entities** may enter into **business associate** agreements with other individuals or organizations to provide services using **PHI** on their behalf. For example, **business associates** might provide accounting services based on **PHI.**

※※※

What kind of information is covered by HIPAA?

Any information collected by a **covered entity** that relates to the past, present, or future physical or mental health condition of an individual; the health care provided to an individual; or the past, present, or future payment for the provision of health care to an individual is **Protected Health Information (PHI)** and therefore subject to the **HIPAA** rule**.** Information also covered under **PHI** includes demographic items such as name, address, and social security number that would allow the identification of an individual (see the glossary for a complete list). The information does not have to be collected or transmitted electronically—information transmitted orally, on paper, or electronically, is **protected health information**.

※※※

What does HIPAA have to do with research?

According to **HIPAA**, research is subject to regulation. "Research" is defined by federal law as: "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge" (45 CFR 164.501). **HIPAA** covers ONLY research that includes health care information as one of its components. **HIPAA** does not replace other federal or state guidelines governing human subjects in research; it supplants those regulations with specific guidelines concerning the privacy of information obtained or created in the course of conducting research.

Covered entities can still conduct their own quality assessments and outcomes and evaluation research outside the **HIPAA** regulations as long as they are not attempting to create generalizable knowledge. If, however, they see their

set with a research organization. A **limited data set** excludes specified direct identifiers of the individual or of their relatives, employers, or household members.

A **data use agreement** must:

1. Establish the permitted uses and disclosures of the **limited data set** by the recipient, consistent with the purposes of the research. Use may not include any disclosure that would violate the Privacy Rule if done by a **covered entity**;

2. Limit who can use or receive the data; and

3. Require the recipient to agree to:

   a. Limit its use or disclosure of the information to the use permitted by the **data use agreement** or as otherwise required by law;

   b. Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the **data use agreement**;

   c. Report to the **covered entity** any use or disclosure of the information not provided for by the **data use agreement** of which the recipient becomes aware;

   d. Ensure that any agents (including subcontractors, to whom the recipient provides the **limited data set**) agree to the same restrictions and conditions that apply to the recipient with respect to the **limited data set**; and

4. Not re-identify the information or contact the study individuals. If a **covered entity** is the recipient of a **limited data set** and violates the **data use**

covered entity (service provider) with the approval it needs to release names and addresses to a researcher for research subject recruitment. Also, if researchers carefully monitor the safety of the **PHI** while conducting their research and maintain the **PHI** no longer than necessary, and the **PHI** elements are necessary to reasonably conduct the research, the criteria for **IRB** approval of a waiver or alteration of authorization have been met.

※※※

Using de-identified data.

De-identified PHI contains no individual identifiers; the identifying data are stripped or removed from a data set by a **covered entity** before the data are provided to researchers. The Privacy Rule allows a **covered entity** to **de-identify data** by removing all **PHI** elements that could be used to identify the individual or the individual's relatives, employers, or household members. The **covered entity** also must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information.

De-identified information is *not* subject to the **HIPAA** Privacy Rule.

※※※

Obtaining a limited data set and data use agreement.

A **limited data set** can be used for purposes of research, public health, or health care operations without the researcher obtaining an individual's authorization for its use or disclosure as long as a **data use agreement** is in place.

The **HIPAA** Privacy Rule allows a **covered entity** to enter into a **data use agreement** for sharing a **limited data**

knowledge base as having usefulness outside their organization, they are likely to be seen as conducting research, particularly if they publish or present their findings to people outside their organization.

When researchers recruit research participants through service providers, identifying residents by name implicitly divulges that a person of that name is receiving a particular type of long-term care service or even is associated with a certain diagnosis. Any information about the services someone is receiving is **protected health information**. There are strategies, however, that will allow researchers to recruit clients through service providers and to conduct research in long-term care settings.

※※※

How can long-term care research be conducted?

There are a number of strategies that can be followed to conduct **HIPAA** compliant research on long-term care services and clients. These are: obtaining authorization from individuals to release **PHI**, obtaining a **waiver of authorization** from the research organization's **Institutional Review Board (IRB)**, using **de-identified data**, or using a **limited data set**. As with many research choices, there are advantages and disadvantages to each of these; the strategy chosen depends upon the research question, the population being studied, and the level of time and effort that the researcher can devote to obtaining health information.

Definition- Institutional Review Board (IRB): An **IRB** is a board or other group designated by an institution to review the legal and ethical aspects of research involving humans as subjects.

※※※

Obtaining authorization from individuals to release PHI.

The most straightforward strategy for release of health information is to obtain written authorization from individuals who are being recruited as research participants. A service provider could recruit research participants and release the names of only those who authorize such a release. They might do this by mailing the researcher's recruitment letter to a group of potential participants. Unfortunately, this is extra effort for service providers and does not allow the researcher to address any questions the clients might have about the study before giving permission. These strategies often result in a lower participation rate than would have been obtained if the researcher approached clients directly.

Written authorization from research participants can be obtained as part of the signed consent form usually required in human subjects research, as long as all of the **authorization elements** are included in the consent form. In general, these elements outline the purpose of the disclosure, the persons to whom, and the conditions under which, **PHI** will be disclosed.

※※※

Obtaining a waiver of authorization.

There are situations in which obtaining written authorization from participants for release of **PHI** is not practical or possible. This is likely to be true when data are centrally gathered about clients who are geographically dispersed, or who will only be contacted by telephone. In these cases an **Institutional Review Board (IRB)** can grant a full or partial **waiver of authorization**. According to the National Institutes of Health, "A complete waiver occurs when an **IRB** determines that a **covered entity** does not need authorization for all **PHI** uses and disclosures for research purposes, such as disclosing **PHI** for research recruitment purposes. An **IRB** may also approve a request that removes some **PHI** but not all, or alters the requirements for an authorization." Thus, a researcher's university **IRB** or a **covered entity's Privacy Board** can grant a waiver or alteration of authorization, provided that the waiver request satisfies the following criteria:

1) The use or disclosure of the **PHI** involves no more than minimal risk, based on the presence of the following elements:

   a. An adequate plan to protect identifiers from improper use and disclosure;

   b. An adequate plan to destroy identifiers at the earliest opportunity (where there is not a research or legal justification for retaining them);

   c. Adequate written assurances that the **PHI** will not be reused or shared with any other person or entity, except as required by law for oversight of the study, or for other research for which the use or disclosure of the **PHI** would be permitted under the Privacy Rule;

2) The research could not feasibly be conducted without the waiver or alteration; and

3) The research could not feasibly be conducted without access to and use of the **PHI**.[1]

This language suggests that an **IRB** can approve the use of **PHI** for research subject recruitment. For example, a university researcher's **IRB** approval can provide the

[1]NIH, August 2003, Institutional Review Boards and the HIPAA Privacy Rule, NIH Pub. No. 03-5428.