Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule

The HIPAA Privacy Rule

Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule and its companion documents explain the Privacy Rule in the research context. They are not intended to be legal documents and should not be construed to be legal advice. The specific Privacy Rule requirements are contained in the relevant laws and regulations.

Preface

This booklet contains information about the "Privacy Rule," a Federal regulation under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 that protects certain health information. The Privacy Rule was issued to protect the privacy of health information that identifies individuals who are living or deceased. The Rule balances an individual's interest in keeping his or her health information confidential with other social benefits, including health care research. This booklet provides researchers with a basic understanding of the Privacy Rule and how it may affect health research. It also addresses how researchers may be directly or indirectly affected by the Rule when their research requires the use of, or access to, an individual's identifiable health information. The Privacy Rule (also known as *Standards for Privacy of Individually Identifiable Health Information)* is in Title 45 of the Code of Federal Regulations, Part 160 and Subparts A and E of Part 164. The full text of the Privacy Rule can be found at the HIPAA Privacy Web site of the Office for Civil Rights (OCR): http://www.hhs.gov/ocr/hipaa.

The Department of Health and Human Services (HHS) issued the Privacy Rule; HHS's OCR has been given the authority to implement and enforce it. To increase researchers' understanding of the Privacy Rule, OCR has developed guidance and technical assistance materials, which can be found at the HIPAA Privacy Web site noted above. In working with OCR, HHS's Office for Human Research Protections (OHRP) and HHS's research agencies, including the Agency for Healthcare Research and Quality (AHRQ), the Centers for Disease Control and Prevention (CDC), the Food and Drug Administration (FDA), and the National Institutes of Health (NIH) have developed Privacy Rule educational materials for the research community. This booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule,* and its companion pieces for clinical, health records, and health services research, and for institutional review boards (IRBs) and Privacy Boards, are part of HHS's ongoing efforts to educate the research community about the Privacy Rule. This booklet and its companion pieces can be found at http://privacyruleandresearch.nih.gov and at the OCR HIPAA Privacy Web site noted above.

Most parties subject to the Privacy Rule must implement the Rule's standards and requirements by April 14, 2003. In addition to accessing the helpful information on the OCR and other Departmental Web sites, researchers should direct questions to their institutions or contact legal counsel about how the Rule may apply to a specific research project or organization. In addition to the information provided in this booklet, other sources of information about the Privacy Rule are listed under "Sources of Information about the Privacy Rule."

Table of Contents

Why Should Researchers Be Aware of the HIPAA Privacy Rule?

The Privacy Rule regulates the way certain health care groups, organizations, or businesses, called covered entities under the Rule, handle the individually identifiable health information known as protected health information (PHI). Researchers should be aware of the Privacy Rule because it establishes the conditions under which covered entities can use or disclose PHI for many purposes, including for research. Although not all researchers will have to comply with the Privacy Rule, the manner in which the Rule protects PHI could affect certain aspects of research.

It is important to understand that many research organizations that handle individually identifiable health information will not have to comply with the Privacy Rule because they will not be covered entities. The Privacy Rule will not directly regulate researchers who are engaged in research within organizations that are not covered entities even though they may gather, generate, access, and share personal health information. For instance, entities that sponsor health research or create and/or maintain health information databases may not themselves be covered entities, and thus may not directly be subject to the Privacy Rule. However, researchers may rely on covered entities for research support or as sources of individually identifiable health information to be included in research repositories or research databases. The Privacy Rule may affect such independent researchers, as it will affect their relationships with covered entities.

In some instances, researchers may have to comply with the Privacy Rule because they may be or may work for a covered entity. For example, the Privacy Rule defines covered entities to include health care providers that transmit health information electronically in connection with certain financial and administrative transactions (such as most hospitals). As such, researchers who are or who work for these covered entities would need to understand the Privacy Rule and how it works because the Rule describes how covered entities can establish relationships in which PHI can be used and shared, as well as the specific ways in which a covered entity may use or disclose the PHI it holds, and under what conditions it can allow use or disclosure of the information.

Researchers in medical and health-related disciplines rely on access to many sources of health information, from medical records and epidemiological databases to disease registries, hospital discharge records, and government compilations of vital and health statistics. For this reason, the Privacy Rule may impact various areas of research, including clinical research, repositories and databases, and health services research. For example, health services researchers study the organization, financing, and delivery of health care services, often by analyzing large databases of health care information maintained by providers, institutions, payers, and government agencies. Clinical researchers often access medical information from patient charts and tissue and data repositories, and create individually identifiable health information in connection with an experimental intervention. For information on how the Privacy Rule may affect specific research areas, see the companion pieces to this booklet: *Health Services Research and the HIPAA Privacy Rule; Repositories, Databases, and the HIPAA Privacy Rule; Clinical Research and the HIPAA Privacy Rule; Institutional Review Boards and the HIPAA Privacy Rule;* and *Privacy Boards and the HIPAA Privacy Rule*.

As you read this booklet, keep in mind that—prior to the Privacy Rule—researchers have been concerned about the privacy accorded to subjects' research-related information and, in fact, may have been required under State and/or Federal laws to take measures to protect such information from inappropriate use and disclosure. The Privacy Rule may add a new layer of privacy protections for those who volunteer for research projects by introducing new ways in which covered entities handle PHI, even for research. This booklet introduces researchers to the Privacy Rule and how covered entities are required to protect individuals' privacy by giving them more comprehensive rights to know and control how and when their PHI is used and disclosed for research. These protections have the potential to strengthen safeguards researchers typically use to protect those who volunteer themselves and their information for advancing medical knowledge.

What Are the Purpose and Background of the Privacy Rule?

Key Points:

- The Privacy Rule establishes minimum Federal standards for protecting the privacy of individually identifiable health information. The Rule confers certain rights on individuals, including rights to access and amend their health information and to obtain a record of when and why their PHI has been shared with others for certain purposes.
- The Privacy Rule establishes conditions under which covered entities can provide researchers access to and use of PHI when necessary to conduct research. The Rule is not intended to impede research.
- Compliance with the Privacy Rule is required on and after April 14, 2003, for most covered entities. (Small health plans have an extra year to comply.)

The purpose of the Privacy Rule is to establish minimum Federal standards for safeguarding the privacy of individually identifiable health information. Covered entities, which must comply with the Rule, are health plans, health care clearinghouses, and certain health care providers. Covered entities may not use or disclose PHI except as permitted or required under the provisions of the Privacy Rule. The Rule also confers certain rights on individuals, including rights to access and amend certain health information and to obtain a record of when and how their PHI has been shared with others for certain purposes. In addition, the Rule establishes administrative requirements for covered entities. Covered entities that fail to comply with the Privacy Rule may be subject to both civil monetary penalties, criminal monetary penalties, and/or imprisonment.

The Privacy Rule recognizes that the research community has legitimate needs to use, access, and disclose individually identifiable health information to carry out a wide range of health research protocols and projects. In the course of conducting research, researchers may create, use, and/or disclose individually identifiable health information. The Privacy Rule protects the privacy of such information when held by a covered entity but also provides various ways in which researchers can access and use the information for research.

The term "Privacy Rule" is often preceded by "HIPAA," an acronym for the Health Insurance Portability and Accountability Act of 1996. The Department of Health and Human Services (HHS) issued the Privacy Rule in December 2000 to carry out HIPAA's mandate that HHS establish Federal standards for safeguarding the privacy of individually identifiable health information. To clarify certain provisions, address unintended negative effects on health care, and relieve unintended administrative burdens, HHS amended the Privacy Rule on August 14, 2002. Most covered entities must comply with the Privacy Rule by April 14, 2003. Small health plans have an extra year, until April 14, 2004, to comply. Entities that become covered entities after these dates must be in compliance with the Privacy Rule at such time that they become covered.

Covered Entity – A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard.

Protected Health Information – PHI is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

Health Information – Any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually Identifiable Health Information – Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Research – A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of research repositories and databases for research.

How Do Other Privacy Protections Interact With the Privacy Rule?

Key Point:

- In addition to the Privacy Rule, State and other Federal laws and regulations, such as HHS regulations for protecting human subjects, continue to govern research when applicable.

State Laws and Regulations

State Law – A constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

In general, the Privacy Rule overrides (or preempts) State laws relating to the privacy of health information that are contrary to the Rule. Any provision of State law that is not contrary to a provision of the Privacy Rule will remain in full force and effect, so that covered entities will continue to have to follow such State laws in addition to the Privacy Rule. However, even where a State law is contrary to the Privacy Rule, there are certain exceptions where the Privacy Rule will not override the contrary State law. For example, State laws that relate to the privacy of individually identifiable health information and are both contrary to and more stringent than the Privacy Rule will continue to stand. In addition, contrary laws and procedures established under State law that provide for reporting of disease or injury, child abuse, birth or death, or for conducting public health surveillance, investigation, and intervention also are not overridden by the Privacy Rule.

Federal Laws and Regulations

The HHS Protection of Human Subjects Regulations – Regulations intended to protect the rights and welfare of human subjects involved in research conducted or supported by HHS.

The FDA Protection of Human Subjects Regulations – Regulations intended to protect the rights, safety, and welfare of participants involved in studies subject to FDA jurisdiction.

Much of the biomedical and behavioral research conducted in the United States is governed either by the rule entitled "Federal Policy for the Protection of Human Subjects" (also known as the "Common Rule," which is codified for HHS at subpart A of Title 45 CFR Part 46)[1,2] and/or the Food and Drug Administration's (FDA) Protection of Human Subjects Regulations at Title 21 CFR Parts 50 and 56.[3] FDA, a component of HHS, has additional human subject protection regulations, which apply to research involving products regulated by FDA. Although these human subject regulatory requirements, which apply to most Federally funded and to some privately funded research, include protections to help ensure the privacy of subjects and the confidentiality of information, the intent of the Privacy Rule, among other things, is to supplement these protections by requiring covered entities to implement specific measures to safeguard the privacy of individually identifiable health information. The Privacy Rule does not replace or act in lieu of these human subject protection regulations, so some researchers who are also (or who work for) covered entities may find themselves responsible for complying with multiple sets of regulations. For purposes of this booklet, some distinctions among the Privacy Rule, the HHS Protection of Human Subjects Regulations, and the FDA Protection of Human Subjects Regulations are outlined.

---

[1] The *Federal Policy for the Protection of Human Subjects* (the "Common Rule" was adopted in 1991 by 15 Federal departments and agencies and was published at 50 *Federal Register* 28002-28032 (1991), and subsequently adopted by the Social Security Administration by Statute and the Central Intelligence Agency by Executive Order.

[2] Title 45 of the *Code of Federal Regulations*, Part 46 at http://ohrp.osophs.dhhs.gov/humansubjects/guidance/45cfr46.htm.

[3] Title 21 of the *Code of Federal Regulations*, Part 50 at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/showCFR.cfm?CFRPart=50&showFR=1, Part 56 at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/showCFR.cfm?CFRPart=56&showFR=1. Additional requirements are found in Title 21 of the *Code of Federal Regulations*, Part 312 at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=312&showFR=1, and Part 812 at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=812&showFR=1.

To the extent that a covered entity is also a Federally assisted drug abuse program, the covered entity is also subject to the Confidentiality of Alcohol and Drug Abuse Patient Records[4] regulation. It may therefore be necessary for covered entities to properly use and disclose individually identifiable health information in compliance with both sets of regulations. Educational materials on the relationship between the Privacy Rule and the Confidentiality of Alcohol and Drug Abuse Patient Records regulation as they relate to research are described in a separate document at the Substance Abuse and Mental Health Administration (SAMHSA) Web site http://www.hipaa.samhsa.gov/.

Certificates of Confidentiality

Certificates of Confidentiality offer an important protection for the privacy of research study participants by protecting identifiable research information from forced disclosure (e.g., through a subpoena or court order). The certificates allow investigators and others with access to research records to refuse to disclose information that could identify research participants in any civil, criminal, administrative, legislative, or other proceeding, whether at the Federal, State, or local level. Certificates of Confidentiality may be granted by the National Institutes of Health (NIH), the Centers for Disease Control and Prevention (CDC), the FDA, and other Federal agencies for studies that collect information that, if disclosed, could damage subjects' financial standing, employability, insurability, or reputation, or have other adverse consequences. By protecting researchers and institutions from forced disclosure of such information, Certificates of Confidentiality help achieve research objectives and promote participation in research studies.

The Privacy Rule and Certificates of Confidentiality afford distinct privacy protections for research subjects. The Privacy Rule does not protect against all forced disclosure since it permits disclosures required by law, for example. Certificates of Confidentiality are legal protections that do protect against forced disclosure by giving their holders a legal basis for refusing to disclose information, which, absent the certificate, they would be obliged to disclose.

Area of Distinction	HIPAA Privacy Rule	HHS Protection of Human Subjects Regulations Title 45 CFR Part 46	FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56
Overall Objective	Establishes a Federal floor of privacy protections for most individually identifiable health information by establishing conditions for its use and disclosure by certain health care providers, health plans, and health care clearinghouses.	To protect the rights and welfare of human subjects involved in research conducted or supported by HHS. Not specifically a privacy regulation.	To protect the rights, safety and welfare of subjects involved in clinical investigations regulated by FDA under 21 U.S.C. 355(i) and 21 U.S.C. 360g(j). Not specifically a privacy regulation.
Applicability	Applies to HIPAA-defined covered entities, regardless of the source of funding.	Applies to human subjects research conducted or supported by HHS.	Applies to research involving products regulated by FDA. Federal support is not necessary for FDA regulations to be applicable. When research subject to FDA jurisdiction is federally funded, both the HHS Protection of Human Subjects Regulations and the FDA Protection of Human Subjects Regulations apply.

[4] Title 42 of the *Code of Federal Regulations*, Part 2 at http://www.access.gpo.gov/nara/cfr/waisidx_02/42cfr2_02.html

To Whom Does the Privacy Rule Apply and Whom Will It Affect?

Key Points:

- The Privacy Rule applies only to covered entities. Many organizations that use, collect, access, and disclose individually identifiable health information will not be covered entities, and thus, will not have to comply with the Privacy Rule.
- The Privacy Rule does not apply to research; it applies to covered entities, which researchers may or may not be. The Rule may affect researchers because it may affect their access to information, but it does not regulate them or research, per se.
- To gain access for research purposes to PHI created or maintained by covered entities, the researcher may have to provide supporting documentation on which the covered entity may rely in meeting the requirements, conditions, and limitations of the Privacy Rule.

The Privacy Rule applies only to covered entities; it does not apply to all persons or institutions that collect individually identifiable health information. It may, however, affect other types of entities that are not directly regulated by the Rule if they, for instance, rely on covered entities to provide PHI. It is important that researchers be aware of how the Rule might affect them in the various types of organizations in which they operate, and what they may have to do in order to continue their research or begin new research efforts on and after the compliance date for the Privacy Rule.

Covered Entities

Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Generally, these transactions concern billing and payment for services or insurance coverage. For example, hospitals, academic medical centers, physicians, and other health care providers who electronically transmit claims transaction information directly or through an intermediary to a health plan are covered entities. Covered entities can be institutions, organizations, or persons.

Researchers are covered entities if they are also health care providers who electronically transmit health information in connection with any transaction for which HHS has adopted a standard. For example, physicians who conduct clinical studies or administer experimental therapeutics to participants during the course of a study must comply with the Privacy Rule if they meet the HIPAA definition of a covered entity.

Health Plan – With certain exceptions, an individual or group plan that provides or pays the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). The law specifically includes many types of organizations and government programs as health plans.

Health Care Clearinghouse – A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches that either process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or receive a standard transaction from another entity and process or facilitate the processing of health information into a nonstandard format or nonstandard data content for the receiving entity.

Health Care Provider – A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Care – Care, services, or supplies related to the health of an individual, including (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Hybrid Entities

Under the Privacy Rule, any entity that meets the definition of a covered entity, regardless of size or complexity, generally will be subject in its entirety to the Privacy Rule. However, the Privacy Rule provides a means by which many covered entities may avoid global application of the Rule, through the hybrid entity designation provisions. This designation will establish which parts of the entity must comply with the Privacy Rule.

Hybrid Entity – A single legal entity that is a covered entity, performs business activities that include both covered and noncovered functions, and designates its health care components as provided in the Privacy Rule. If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components. However, non-health care components of a hybrid entity may be affected because the health care component is limited in how it can share PHI with the non-health care component. The covered entity also retains certain oversight, compliance, and enforcement responsibilities.

Any single legal entity may elect to be a hybrid entity if it performs both covered and noncovered functions as part of its business operations. A covered function is any function the performance of which makes the performer a health plan, a health care provider, or a health care clearinghouse. To become a hybrid entity, the covered entity must designate the health care components within its organization. Health care components must include any component that would meet the definition of covered entity if that component were a separate legal entity. A health care component may also include any component that conducts covered functions (i.e., noncovered health care provider) or performs activities that would make the component a business associate of the entity if it were legally separate. Within a hybrid entity, most of the requirements of the Privacy Rule apply only to the health care component(s), although the covered entity retains certain oversight, compliance, and enforcement obligations.

For example, a university may be a single legal entity that includes an academic medical center's hospital that conducts electronic transactions for which HHS has adopted standards. Because the hospital is part of the legal entity, the whole university, including the hospital, will be a covered entity. However, the university may elect to be a hybrid entity. To do so, it must designate the hospital as a health care component. The university also has the option of including in the designation other components that conduct covered functions or business associate-like functions. Most of the Privacy Rule's requirements would then only apply to the hospital portion of the university and any other designated components. The Privacy Rule would govern only the PHI created, received, or maintained by, or on behalf of, these components. PHI disclosures by the hospital to the rest of the university are regulated by the Privacy Rule in the same way as disclosures to entities outside the university.

Research components of a hybrid entity that function as health care providers and conduct certain standard electronic transactions must be included in the hybrid entity's health care component(s) and be subject to the Privacy Rule. However, research components that function as health care providers, but do not conduct these electronic transactions may, but are not required to, be included in the health care component(s) of the hybrid entity. For example, if the university in the example above also has a research laboratory that functions as a health care provider but does not engage in specified electronic transactions, the university as a hybrid entity has the option to include or exclude the research laboratory from its health care component. If such a research laboratory is included in the hybrid entity's health care component, then the employees or workforce members of the laboratory must comply with the Privacy Rule. But if the research laboratory is excluded from the hybrid entity's health care component, the employees or workforce members of the laboratory are effectively not subject to the Privacy Rule.

The hybrid entity is not permitted, however, to include in its health care component, a research component that does not function as a health care provider or does not conduct business associate-like functions. For example, a research component that conducts purely records research is not performing covered or business associate-like functions and, thus, cannot be included in the hybrid entity's health care component.

Business Associates

The Privacy Rule also protects individually identifiable health information when it is created or maintained by a person or entity conducting certain functions on behalf of a covered entity—a business associate. A business associate is a person or entity, who is not a member of the workforce and performs or assists in performing, for or on behalf of a covered entity, a function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule, involving the use or disclosure of individually identifiable health information, or that provides certain services to a covered entity that involve the use or disclosure of individually identifiable health information. Because the HIPAA Administrative Simplification Rules do not directly regulate research activities, the Privacy Rule does not require a researcher or a research sponsor to become a business associate of a covered entity for research purposes. However, a covered entity may engage business associates to assist in de-identifying PHI, to prepare limited data sets, or to perform data aggregation. The Privacy Rule requires a covered entity to enter into a written contract, or another arrangement permitted by the Rule if both parties are government entities, with its business associates. The Rule's business associate provisions can be found in Sections 164.502(e) and 164.504(e). Generally, a covered entity may, for the purposes permitted by the Privacy Rule and specified in its written agreement with its business associate, disclose PHI to that business associate and allow the business associate to use, create, or receive PHI on its behalf. Before the covered entity discloses the PHI to the business associate, the covered entity must obtain satisfactory assurances, generally in the form of a contract, that the business associate will appropriately safeguard the information. With a few limited exceptions, the contract may not authorize the business associate to use or further disclose the PHI in a manner that would violate the Privacy Rule if done directly by the covered entity.

Business Associate – A person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, or any other function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule. Business associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of individually identifiable health information by the covered entity or another business associate of the covered entity to that person or entity. A member of a covered entity's workforce is not one of its business associates. A covered entity may be a business associate of another covered entity.

Determining Your Status Under the Privacy Rule

The determination of whether an individual researcher must comply with the Privacy Rule is a fact-sensitive, individualized determination. The answer to this question may depend on how the entity with which a researcher has a relationship is organized. Questions on a researcher's status under the Privacy Rule should be referred to the appropriate representatives within that organization. Neither the Federal Government nor this booklet makes, or should be construed to make, this determination.

HHS has developed a set of tools to help an entity determine whether it is a health plan, a health care clearinghouse, or a covered health care provider that will be subject to the Privacy Rule. These tools are available at the following link:

http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.

What Health Information Is Protected by the Privacy Rule?

Key Points:

- With certain exceptions, the Privacy Rule protects a subset of individually identifiable health information, known as protected health information or PHI, that is held or maintained by covered entities or their business associates acting for the covered entity.
- The Privacy Rule does not protect individually identifiable health information that is held or maintained by entities other than covered entities or business associates that create, use, or receive such information on behalf of the covered entity.

To understand the possible impact of the Privacy Rule on their work, researchers will need to understand what individually identifiable health information is and is not protected under the Rule. With certain exceptions, the Privacy Rule protects a certain type of individually identifiable health information, created or maintained by covered entities and their business associates acting for the covered entity. This information is known as "protected health information" or PHI.

The Privacy Rule defines PHI as individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity, that is transmitted or maintained in any form or medium (including the individually identifiable health information of non-U.S. citizens). This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse. For purposes of the Privacy Rule, genetic information is considered to be health information.

There are, however, instances when individually identifiable health information held by a covered entity is not protected by the Privacy Rule. The Rule excludes from the definition of PHI individually identifiable health information that is maintained in education records covered by the Family Educational Right and Privacy Act (as amended, 20 U.S.C. 1232g) and records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records containing individually identifiable health information that are held by a covered entity in its role as an employer.

A critical point of the Privacy Rule is that it applies only to individually identifiable health information held or maintained by a covered entity or its business associate acting for the covered entity. Individually identifiable health information that is held by anyone other than a covered entity, including an independent researcher who is not a covered entity, is not protected by the Privacy Rule and may be used or disclosed without regard to the Privacy Rule. There may, however, be other Federal and State protections covering the information held by these entities that limit its use or disclosure.

When health information is individually identifiable and is held by a covered entity, it is likely to be PHI. In contrast, the HHS Protection of Human Subjects Regulations describe "private information" as including information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record). Under the HHS Protection of Human Subjects Regulations, private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects unless data are obtained through intervention or interaction with the individual.

Area of Distinction	HIPAA Privacy Rule	HHS Protection of Human Subjects Regulations Title 45 CFR Part 46	FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56
Identifiable Information	Defines PHI as individually identifiable health information that is transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records.	Private information must be individually identifiable in order for obtaining the information to constitute research involving human subjects. Individually identifiable means the identity of the subject is or may readily be ascertained by the investigator or associated with the information.	Title 21 CFR Parts 50 and 56 do not define individually identifiable health information.

How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?

Key Points:

- De-identified health information, as described in the Privacy Rule, is not PHI, and thus is not protected by the Privacy Rule.
- PHI may be used and disclosed for research with an individual's written permission in the form of an Authorization.
- PHI may be used and disclosed for research without an Authorization in limited circumstances: Under a waiver of the Authorization requirement, as a limited data set with a data use agreement, preparatory to research, and for research on decedents' information.

The Privacy Rule describes the ways in which covered entities can use or disclose PHI, including for research purposes. In general, the Rule allows covered entities to use and disclose PHI for research if authorized to do so by the subject in accordance with the Privacy Rule. In addition, in certain circumstances, the Rule permits covered entities to use and disclose PHI without Authorization for certain types of research activities. For example, PHI can be used or disclosed for research if a covered entity obtains documentation that an Institutional Review Board (IRB) or Privacy Board has waived the requirement for Authorization or allowed an alteration. The Rule also allows a covered entity to enter into a data use agreement for sharing a limited data set. There are also separate provisions for how PHI can be used or disclosed for activities preparatory to research and for research on decedents' information.

It is important to note that there are circumstances in which health information maintained by a covered entity is not protected by the Privacy Rule. PHI excludes health information that is de-identified according to specific standards. Health information that is de-identified can be used and disclosed by a covered entity, including a researcher who is a covered entity, without Authorization or any other permission specified in the Privacy Rule. Under the Privacy Rule, covered entities may determine that health information is not individually identifiable in either of two ways. These are described below.

De-identifying Protected Health Information Under the Privacy Rule

Covered entities may use or disclose health information that is de-identified without restriction under the Privacy Rule. Covered entities seeking to release this health information must determine that the information has been de-identified using either statistical verification of de-identification or by removing certain pieces of information from each record as specified in the Rule.

The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members; these elements are enumerated in the Privacy Rule. 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. Under this method, the identifiers that must be removed are the following:

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
   a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
   b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

Covered entities may also use statistical methods to establish de-identification instead of removing all 18 identifiers. The covered entity may obtain certification by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" that there is a "very small" risk that the information could be used by the recipient to identify the individual who is the subject of the information, alone or in combination with other reasonably available information. The person certifying statistical de-identification must document the methods used as well as the result of the analysis that justifies the determination. A covered entity is required to keep such certification, in written or electronic format, for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

Other Issues Relating to De-identification

Under the first method, unique identifying numbers, characteristics, or codes must be removed if the health information is to be considered de-identified. However, the Privacy Rule permits a covered entity to assign to, and retain with, the health information a code or other means of record identification if that code is not derived from or related to the information about the individual and could not be translated to identify the individual. The covered entity may not use or disclose the code or other means of record identification for any other purpose and may not disclose its method of re-identifying the information. For example, a randomly assigned code that permits re-identification through a secured key to that code would not make the information to which it is assigned PHI, because a random code would not be derived from or related to information about the individual and because the key to that code is secure.

A covered entity is permitted to de-identify PHI or engage a business associate to de-identify PHI. For example, a researcher may be a covered entity him/herself performing, or may be hired as a business associate to perform, the de-identification. In most cases, the covered entity must have a written contract with the business associate containing the provisions required by the Privacy Rule before it provides PHI to the business associate. In addition, a covered entity, if a hybrid entity, could designate in its health care component(s) portions of the entity that conduct business associate-like functions, such as de-identification.

De-identifying PHI according to Privacy Rule standards may enable many research activities; however, the Privacy Rule recognizes that researchers may need access to and generate identifiable health information during the course of research. Where PHI is needed for research activities, the Privacy Rule permits its use and disclosure if certain standards are met. These standards are discussed in the following sections.

Authorization for Research Uses and Disclosures

One way the Privacy Rule protects the privacy of PHI is by generally giving individuals the opportunity to agree to the uses and disclosures of their PHI by signing an Authorization form for uses and disclosures not otherwise permitted by the Rule. The Privacy Rule establishes the right of an individual, such as a research subject, to authorize a covered entity to use and disclose his/her PHI for research purposes. This requirement is in addition to the informed consent to participate in research required under the HHS Protection of Human Subjects Regulations and other applicable Federal and State law.

Area of Distinction	HIPAA Privacy Rule	HHS Protection of Human Subjects Regulations Title 45 CFR Part 46	FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56
Permissions for Research	Authorization	Informed Consent	Informed Consent
IRB/Privacy Board Responsibilities	Requires the covered entity to obtain Authorization for research use or disclosure of PHI unless a regulatory permission applies. Because of this, the IRB or Privacy Board would only see requests to waive or alter the Authorization requirement. In exercising Privacy Rule authority, the IRB or Privacy Board does not review the Authorization form.	The IRB must ensure that informed consent will be sought from, and documented for, each prospective subject or the subject's legally authorized representative, in accordance with, and to the extent required by, HHS regulations. If specified criteria are met, the IRB may waive the requirements for either obtaining informed consent or documenting informed consent. The IRB must review and approve the Authorization form if it is combined with the informed consent document. Privacy Boards have no authority under the HHS Protection of Human Subjects Regulations.	The IRB must ensure that informed consent will be sought from, and documented for, each prospective subject or the subject's legally authorized representative, in accordance with, and to the extent required by, FDA regulations. If specified criteria are met, the requirements for either obtaining informed consent or documenting informed consent may be waived. The IRB must review and approve the Authorization form if it is combined with the informed consent document. Privacy Boards have no authority under the FDA Protection of Human Subjects Regulations.

Elements of an Authorization

A valid Privacy Rule Authorization is an individual's signed permission that allows a covered entity to use or disclose the individual's PHI for the purposes, and to the recipient or recipients, as stated in the Authorization. When an Authorization is obtained for research purposes, the Privacy Rule requires that it pertain only to a specific research study, not to nonspecific research or to future, unspecified projects. The Privacy Rule considers the creation and maintenance of a research repository or database as a specific research activity, but the subsequent use or disclosure by a covered entity of information from the database for a specific research study will require separate Authorization unless the PHI use or disclosure is permitted without Authorization (discussed later in this section). If an Authorization for research is obtained, the actual uses and disclosures made must be consistent with what is stated in the Authorization. The signed Authorization must be retained by the covered entity for 6 years from the date of creation or the date it was last in effect, whichever is later.

An Authorization differs from an informed consent in that an Authorization focuses on privacy risks and states how, why, and to whom the PHI will be used and/or disclosed for research. An informed consent, on the other hand, provides research subjects with a description of the study and of its anticipated risks and/or benefits, and a description of how the confidentiality of records will be protected, among other things. An Authorization can be combined with an informed consent document or other permission to participate in research. Whether combined with an informed consent or separate, an Authorization must contain the following specific core elements and required statements stipulated in the Rule:

Authorization Core Elements:

- A description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner.
- The names or other specific identification of the person or persons (or class of persons) authorized to make the requested use or disclosure.
- The names or other specific identification of the person or persons (or class of persons) to whom the covered entity may make the requested use or disclosure.
- A description of each purpose of the requested use or disclosure.
- Authorization expiration date or expiration event that relates to the individual or to the purpose of the use or disclosure ("end of the research study" or "none" are permissible for research, including for the creation and maintenance of a research database or repository).
- Signature of the individual and date. If the individual's legally authorized representative signs the Authorization, a description of the representative's authority to act for the individual must also be provided.

Authorization Required Statements:

- A statement of the individual's right to revoke his/her Authorization and how to do so, and, if applicable, the exceptions to the right to revoke his/her Authorization or reference to the corresponding section of the covered entity's notice of privacy practices.
- Whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on Authorization, including research-related treatment and consequences of refusing to sign the Authorization, if applicable.
- A statement of the potential risk that PHI will be re-disclosed by the recipient. This may be a general statement that the Privacy Rule may no longer protect health information disclosed to the recipient.

The Privacy Rule does not specify who may draft the Authorization, so a researcher could draft it regardless of whether the researcher is a covered entity. However, in order to have a Privacy Rule-compliant Authorization, it must be written in plain language and contain the core elements and required statements, and a signed copy must be provided to the individual signing it if the covered entity itself is seeking the Authorization. The companion piece *Sample Authorization Language* contains language that illustrates the inclusion of core elements and required statements.

NOTE: If an Authorization permits disclosure of the individual's PHI to a person or organization that is not a covered entity or a business associate acting on behalf of a covered entity (such as a sponsor or funding source of the research), the Privacy Rule does not continue to protect the PHI disclosed to such entity. However, other applicable Federal and State laws between the disclosing covered entity and the PHI recipient may establish continuing protections for the disclosed information. Under the HHS Protection of Human Subjects Regulations or the FDA Protection of Human Subjects Regulations, an IRB may impose further restrictions on the use or disclosure of research information to protect subjects.

An Authorization for research uses and disclosures need not have a fixed expiration date or state a specific expiration event; the form can list "none" or "the end of the research project." However, although an Authorization for research uses and disclosure need not expire, a research subject has the right to revoke, in writing, his/her Authorization at any time. The individual's revocation is effective, except to the extent that the covered entity has taken action in reliance upon the Authorization prior to revocation. For example, a covered entity is not required to retrieve information that it disclosed under a valid Authorization before learning of the revocation. And the preamble to the Privacy Rule states that, for research uses and disclosures, the reliance exception would permit the continued use and disclosure of PHI already obtained with an Authorization to the extent necessary to protect the integrity of the research—for example, to account for a subject's withdrawal from the research study, to conduct investigations of scientific misconduct, or to report adverse events.

Waiver or Alteration of the Authorization Requirement

Many health research projects and protocols cannot be undertaken using health information that has been de-identified. Also, it may not be feasible for a researcher to obtain a signed Authorization for all PHI the researcher needs to obtain for the research study. In other cases, a researcher may determine that consents obtained prior to April 14, 2003, that permit the use and disclosure of information obtained from research subjects are inadequate, insufficient, or restrict the research protocol or procedure such that an Authorization may be necessary to permit the PHI use or disclosure for the research.

To address these and other situations that may arise in the course of a research project or protocol, the Privacy Rule contains criteria for waiver or alterations of Authorizations by an IRB or another review body called a Privacy Board. Many of the provisions were modeled on the HHS Protection of Human Subjects Regulations. The Privacy Rule does not change current requirements that specify when researchers must submit protocols to the IRB for review and approval, and obtain informed consent documents. The Privacy Rule adds to such requirements only when a researcher requests a waiver or an alteration of Authorization. If a covered entity has used or disclosed PHI for research with an IRB or Privacy Board approval of waiver or alteration of Authorization, documentation of that approval must be retained by the covered entity for 6 years from the date of its creation or the date it was last in effect, whichever is later.

For research uses and disclosures of PHI, an IRB or Privacy Board may approve a waiver or an alteration of the Authorization requirement in whole or in part. A complete waiver occurs when the IRB or Privacy Board determines that no Authorization will be required for a covered entity to use and disclose PHI for a particular research project. A partial waiver of Authorization occurs when an IRB or Privacy Board 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 or Privacy Board may also approve a request that removes some PHI, but not all, or alters the requirements for an Authorization (an alteration).

The Privacy Rule does not alter IRB membership requirements, jurisdiction on matters concerning the protection of human subjects, or other procedural IRB matters. The Privacy Rule states that the required documentation must indicate that the IRB followed normal or expedited procedures in reviewing and approving the waiver or alteration. Thus, an IRB's authority to act on waiver or alteration requests under the Privacy Rule is in addition to the other authorities derived from the HHS Protection of Human Subjects Regulations and other applicable statutes and regulations. The process and criteria for obtaining a waiver of Authorization under the Privacy Rule is similar to the process and criteria for waiving informed consent in the HHS Protection of Human Subjects Regulations. Additional information on the Privacy Rule and IRBs can be found in the companion piece entitled *Institutional Review Boards and the HIPAA Privacy Rule*.

Privacy Boards are new, alternative review boards authorized by the Privacy Rule to review requests for alteration or waiver of a research Authorization. If a covered entity is to use or disclose PHI on the basis of a waiver or an alteration of Authorization from a Privacy Board, the Board must be established in accordance with Section 164.512(i) of the Privacy Rule. These provisions state that:

- Members must have varying backgrounds and appropriate professional competencies as necessary to review the effect of the research protocol on individuals' privacy rights and related interests.
- Each Board must have at least one member who is not affiliated with the covered entity or with any entity conducting or sponsoring the research and who is not related to any person who is affiliated with such entities.
- Members may not have conflicts of interest regarding the projects they review.

Additional information on the Privacy Rule and Privacy Boards can be found in the companion piece entitled *Privacy Boards and the HIPAA Privacy Rule*.

Documentation of the waiver or alteration of Authorization must include a statement identifying the IRB or Privacy Board that made the approval and the date of approval. Among other things, the documentation must also include statements that the IRB or Privacy Board has determined that the waiver or alteration of Authorization, in whole or in part, satisfies the following criteria:

1. The use or disclosure of the PHI involves no more than minimal risk to the privacy of individuals based on, at least, the presence of the following elements:
   a. An adequate plan to protect health information identifiers from improper use and disclosure.
   b. An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research (absent a health or research justification for retaining them or a legal requirement to do so).
   c. Adequate written assurances that the PHI will not be reused or disclosed to (shared with) any other person or entity, except as required by law, for authorized oversight of the research 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 practicably be conducted without the waiver or alteration.
3. The research could not practicably be conducted without access to and use of the PHI.

The Privacy Rule does not require an IRB or Privacy Board to review the form or content of the Authorization a researcher or covered entity intends to use, or the proposed uses and disclosures of PHI made according to an Authorization. Under the Privacy Rule, an IRB or Privacy Board need only review requests to waive or alter the Authorization requirement.

Many research projects take place at multiple sites and/or require the use and disclosure of PHI created or maintained by more than one covered entity (collectively, *multisite projects*). Often, different IRBs are involved in multisite project reviews. The same situation is expected to occur with Privacy Boards. In some circumstances, Privacy Boards and IRBs will coexist. Where these boards coexist, the Privacy Rule does *not* require approval of a waiver or an alteration of Authorization by both bodies because a covered entity may rely on a waiver or an alteration of Authorization approved by any IRB or Privacy Board, without regard to the location of the approver.

HHS has stated (65 *Federal Register* 82692, December 28, 2000) that a covered entity's responsibility is to "obtain the documentation that *one* [emphasis added] IRB or privacy board has approved the alteration or waiver of Authorization." Consequently, the Privacy Rule allows a waiver or an alteration of Authorization obtained from a single IRB or Privacy Board to be used to obtain PHI in connection with a multisite project. However, HHS also recognizes that "covered entities may elect to require duplicate IRB or Privacy Board reviews before disclosing [PHI] to requesting researchers" (67 *Federal Register* 53232, August 14, 2002). While the Privacy Rule does not address potential splits between IRBs and Privacy Boards, HHS "strongly encourages researchers to notify IRBs and privacy boards of any prior IRB or privacy board review of a research protocol" (65 *Federal Register* 82692, December 28, 2000).

Area of Distinction	HIPAA Privacy Rule	HHS Protection of Human Subjects Regulations Title 45 CFR Part 46	FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56
Review of Cooperative Research	Requests to waive or alter the Authorization requirement are reviewed and approved by an IRB or Privacy Board. The Privacy Rule permits a covered entity to reasonably rely on the determination of an IRB or Privacy Board, if the covered entity obtains appropriate documentation of such determination.	Each institution is responsible for safeguarding the rights and welfare of human subjects and for complying with the HHS Protection of Human Subjects Regulations. With the approval of HHS, an institution participating in a cooperative project may enter into a joint review arrangement, rely upon the review of another qualified IRB, or make similar arrangements for avoiding duplication of effort.	Cooperative research/multi-institutional studies may use joint review, reliance upon the review of another qualified IRB, or similar arrangements aimed at avoiding duplication of effort.

Area of Distinction	HIPAA Privacy Rule	HHS Protection of Human Subjects Regulations Title 45 CFR Part 46	FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56
Waivers of Authorization or Informed Consent Requirements	Allows waiver or alteration of Authorization when IRB or Privacy Board deems the following criteria are met: (1) Use or disclosure involves no more than minimal risk to the privacy of individuals because of the presence of at least the following elements: (a) An adequate plan to protect health information identifiers from improper use or disclosure, (b) an adequate plan to destroy identifiers at the earliest opportunity absent a health or research justification or legal requirement to retain them, and (c) adequate written assurances that the PHI will not be used or disclosed to a third party except as required by law, for authorized oversight of the research study, or for other research uses and disclosures permitted by the Privacy Rule; (2) research could not practicably be conducted without the waiver or alteration; and (3) research could not practicably be conducted without access to and use of PHI.	Permits an IRB to waive some or all of the elements of informed consent, or to waive the requirement to obtain informed consent, provided the IRB finds and documents that (1) the research involves no more than minimal risk to the subjects; (2) the waiver or alteration will not adversely affect the rights and welfare of the subjects; (3) the research could not practicably be carried out without the waiver or alteration; and (4) whenever appropriate, the subjects will be provided with additional pertinent information after participation. Permits an IRB to waive the requirement for the investigator to obtain a signed consent for some or all of the subjects if it finds either (1) that the only record linking the subject and the research would be the consent document and the principal risk would be potential harm resulting from a breach of confidentiality; or (2) that the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.	Permits FDA to waive the IRB review requirement. Permits an IRB to approve a clinical investigation without subjects' informed consent in certain circumstances specified in 21 CFR 50.23 and 21 CFR 50.24. These include (1) circumstances in which immediate use of the test article is, in the investigator's opinion, required to preserve the life of the subject, and time is not sufficient to obtain informed consent; (2) circumstances when the U.S. President may waive informed consent for military personnel for administration of an investigational product to members of the armed forces; and (3) circumstances involving emergency research.

Limited Data Set and Data Use Agreement

The Privacy Rule permits a covered entity, without obtaining an Authorization or documentation of a waiver or an alteration of Authorization, to use and disclose PHI included in a limited data set. A covered entity may use and disclose a limited data set for research activities conducted by itself, another covered entity, or a researcher who is not a covered entity if the disclosing covered entity and the limited data set recipient enter into a data use agreement. Limited data sets may be used or disclosed only for purposes of research, public health, or health care operations. Because limited data sets may contain identifiable information, they are still PHI.

Limited Data Set – Refers to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's Authorization or a waiver or an alteration of Authorization for its use and disclosure, with a data use agreement.

Data Use Agreement – An agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

A limited data set is described as health information that excludes certain, listed direct identifiers (see below) but that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed in the Privacy Rule's limited data set provisions apply both to information about the individual and to information about the individual's relatives, employers, or household members. The following identifiers must be removed from health information if the data are to qualify as a limited data set:

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face photographic images and any comparable images.

A data use agreement is the means by which covered entities obtain satisfactory assurances that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes. Even if the person requesting a limited data set from a covered entity is an employee or otherwise a member of the covered entity's workforce, a written data use agreement meeting the Privacy Rule's requirements must be in place between the covered entity and the limited data set recipient.

The Privacy Rule requires a data use agreement to contain the following provisions:

- Specific permitted uses and disclosures of the limited data set by the recipient consistent with the purpose for which it was disclosed (a data use agreement cannot authorize the recipient to use or further disclose the information in a way that, if done by the covered entity, would violate the Privacy Rule).
- Identify who is permitted to use or receive the limited data set.
- Stipulations that the recipient will
  - Not use or disclose the information other than permitted by the agreement or otherwise required by law.
  - Use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement, and require the recipient to report to the covered entity any uses or disclosures in violation of the agreement of which the recipient becomes aware.
  - Hold any agent of the recipient (including subcontractors) to the standards, restrictions, and conditions stated in the data use agreement with respect to the information.
  - Not identify the information or contact the individuals.

If a covered entity is the recipient of a limited data set and violates the data use agreement, it is deemed to have violated the Privacy Rule. If the covered entity providing the limited data set knows of a pattern of activity or practice by the recipient that constitutes a material breach or violation of the data use agreement, the covered entity must take reasonable steps to correct the inappropriate activity or practice. If the steps are not successful, the covered entity must discontinue disclosure of PHI to the recipient and notify HHS.

Section 164.512 of the Privacy Rule also establishes specific PHI uses and disclosures that a covered entity is permitted to make for research without an Authorization, a waiver or an alteration of Authorization, or a data use agreement. These limited activities are the use or disclosure of PHI preparatory to research and the use or disclosure of PHI pertaining to decedents for research.

Activities Preparatory to Research

For activities involved in preparing for research, covered entities may use or disclose PHI to a researcher without an individual's Authorization, a waiver or an alteration of Authorization, or a data use agreement. However, the covered entity must obtain from a researcher representations that (1) the use or disclosure is requested solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research, (2) the PHI will not be removed from the covered entity in the course of review, and (3) the PHI for which use or access is requested is necessary for the research. The covered entity may permit the researcher to make these representations in written or oral form.

According to HHS guidance on the Privacy Rule,

> The preparatory to research provision permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. However, the provision at 45 CFR 164.512(i)(1)(ii) does not permit the researcher to remove protected health information from the covered entity's site. *As such, a researcher who is an employee or a member of the covered entity's workforce could use protected health information to contact prospective research subjects* [emphasis added]. The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their Authorization to use or disclose protected health information for a research study.

Under the preparatory to research provision, a covered entity may permit a researcher who works for that covered entity to use PHI for purposes preparatory to research. A covered entity may also permit, as a disclosure of PHI, a researcher who is not a workforce member of that covered entity to review PHI (within that covered entity) for purposes preparatory to research. Within a hybrid entity, the situation is similar. A covered entity that is a hybrid entity may permit a researcher within its health care component to use, without an individual's Authorization, PHI for activities preparatory to research. A covered entity may also permit a researcher who is outside the hybrid entity's health care component to review PHI within that health care component without an individual's Authorization for purposes preparatory to research.

Researchers should note that any preparatory research activities involving human subjects research as defined by the HHS Protection of Human Subjects Regulations, which are not otherwise exempt, must be reviewed and approved by an IRB and must satisfy the informed consent requirements of HHS regulations.

Research on Decedents' Protected Health Information

To use or disclose PHI of the deceased for research, covered entities are not required to obtain Authorizations from the personal representative or next of kin, a waiver or an alteration of the Authorization, or a data use agreement. However, the covered entity must obtain from the researcher who is seeking access to decedents' PHI (1) oral or written representations that the use and disclosure is sought solely for research on the PHI of decedents, (2) oral or written representations that the PHI for which use or disclosure is sought is necessary for the research purposes, and (3) documentation, at the request of the covered entity, of the death of the individuals whose PHI is sought by the researchers.

Other Uses and Disclosures of Protected Health Information

Some of the PHI uses and disclosures that are permitted under the Privacy Rule at Section 164.512 without Authorization, waiver or alteration of Authorization, or data use agreement are summarized below. Covered entities seeking to use and disclose PHI for these or other purposes permitted under Section 164.512 should consult the Privacy Rule for information on the relevant implementation requirements.

Among other limited purposes, a covered entity may use or disclose PHI without an Authorization, as follows:

- To the extent the use or disclosure is required by law and complies with, and is limited to, the relevant requirements of such law. For example, a covered entity may disclose, without Authorization, PHI to cancer registries if the disclosure (or reporting) is required by law. In addition,

a covered entity may disclose to the Federal Government, without Authorization, PHI associated with data first produced under a Federal award in accordance with 45 CFR 74.36[5].

- For disclosure to a public health authority that is authorized by law to collect or receive the information for purposes of preventing or controlling disease, injury, or disability. Activities included here are reporting disease, injury, and vital events, such as birth or death, as well as conducting public health surveillance, investigations, and interventions. For example, a covered entity may disclose PHI, without Authorization, related to an adverse event to NIH or FDA as public health authorities. Additional guidance on the use and disclosure of PHI for public health purposes is available at: Centers for Disease Control and Prevention (2003). HIPPA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services. *Morbidity and Mortality Weekly Report,* 52.
- To a person subject to the jurisdiction of the FDA with respect to an FDA-regulated product or activity for which that person has responsibility, for purposes related to the quality, safety, or effectiveness of the FDA-regulated product or activity (including, but not limited to, adverse event reporting; FDA-regulated product tracking; post-marketing surveillance; and enabling product recalls, repairs, replacements, or lookback). For example, a covered entity may disclose adverse event/safety reports to sponsors of investigational new products.
- To health oversight agencies for oversight activities authorized by law that are necessary, for example, for the appropriate oversight of government-regulated programs. For example, because Office for Human Research Protections (OHRP) is a health oversight agency under the Privacy Rule, a covered entity may disclose PHI, without Authorization, to OHRP for purposes of determining compliance with the HHS Protection of Human Subjects Regulations.

Minimum Necessary Restriction

With some exceptions, the Privacy Rule imposes a minimum necessary requirement on all permitted uses and disclosures of PHI by a covered entity. This means that a covered entity must apply policies and procedures, or criteria it has developed, to limit certain uses or disclosures of PHI, including those for research purposes, to "the information reasonably necessary to accomplish the purpose [of the sought or requested use or disclosure]." For uses and routine and recurring disclosures of and requests for PHI, the covered entity must develop policies and procedures (which may be standard protocols) to reasonably limit such uses, disclosures, and requests to the minimum necessary to achieve the purpose of the use or disclosure. For nonroutine disclosures and requests, a covered entity must review each disclosure or request individually against criteria it has developed.

There are several exceptions to the minimum necessary requirements that may affect researchers (Sections 164.502(b) and 164.514(d) of the Privacy Rule). The minimum necessary standard does not apply to the following:

- Uses and disclosures made with an individual's Authorization.
- Disclosures to, or requests by, a health care provider for treatment.
- Disclosures to the individual.
- Uses or disclosures required by law.
- Disclosures to HHS for purposes of determining compliance with the Privacy Rule.
- When required for compliance with other HIPAA rules (e.g., to fill out required or situationally required data fields in standard transactions).

Unless otherwise excepted, covered entities are required to implement policies and procedures or establish criteria that limit the PHI used, disclosed, or requested to the minimum amount reasonably necessary to achieve the purposes (e.g., necessary for the specific research) for which disclosure is sought. These covered entity policies

[5] Title 45 of the *Code of Federal Regulations*, Part 74.36 at http://www.access.gpo.gov/nara/cfr/waisidx_01/45cfr74_01.html

and procedures will apply to researchers who are members of the covered entity's workforce and may apply to business associates.

The Privacy Rule does not require a covered entity to independently determine, in all instances, whether a request for PHI meets the minimum necessary requirement. As relevant here, the Privacy Rule permits the covered entity to rely, when reasonable, on a request for disclosure of PHI as the minimum necessary when making permitted disclosures to public officials, disclosing information requested by another covered entity, or when disclosing PHI to researchers who have documentation of an IRB or Privacy Board waiver or alteration of Authorization or certain other representations permitted by the Privacy Rule, which are discussed in detail in related publications, *Institutional Review Boards and the HIPAA Privacy Rule* and *Privacy Boards and the HIPAA Privacy Rule*.

How Are Research Subjects' Rights Affected by the Privacy Rule?

Key Points:

- The Privacy Rule provides individuals with certain rights about how their health information is used and disclosed as well as how they can gain access to health records and information about when their PHI was released without their permission.
- The Privacy Rule describes how covered entities can implement these rights while maintaining the integrity of the research project.

In addition to establishing conditions for the use and disclosure of PHI, the Privacy Rule establishes certain rights of individuals with respect to their health information. Covered entities must provide individuals with written notice of the entity's privacy practices and the individual's privacy rights. In addition, the Rule permits individuals to gain access to, request amendment of, request restrictions on, and request confidential communication of certain records related to their health care. Individuals are also given the right to request and receive a written account from a covered entity of when and why their PHI has been disclosed without their Authorization, except under limited circumstances. Individuals also have the right to complain to the covered entity and to the Secretary of Health and Human Services if they believe a violation of the Privacy Rule has occurred. This document discusses an individual's rights to access PHI and receive an accounting of PHI disclosures.

Access to Protected Health Information

With few exceptions, the Privacy Rule guarantees individuals access to their medical records and other types of health information to the extent the information is maintained by the covered entity or its business associate within a designated record set. Research records maintained by a covered entity may be part of a designated record set if, for example, the records are medically related or are used to make decisions about research participants.

Designated Record Set – A group of records maintained by or for a covered entity that includes (1) medical and billing records about individuals maintained by or for a covered health care provider; (2) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for the covered entity to make decisions about individuals. A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

In most cases, patients or research subjects can have access to their health information in a designated record set at a convenient time and place. One exception, among others, is during a clinical trial, when the individual's right of access can be suspended while the research is in progress if, in consenting to participate in research including treatment, the individual agreed to the temporary denial of access. The covered entity, however, must inform the individual that the right to access his/her health records in the designated record set will be restored upon conclusion of the clinical trial.

Accounting of Disclosures of Protected Health Information

The Privacy Rule permits individuals to obtain a record of certain disclosures of their PHI by covered entities or their business associates, including certain disclosures made by researchers who must comply with the Rule. This is known as an accounting of disclosures. It is important to emphasize the difference between a use and a disclosure of PHI. In general, the use of PHI means communicating that information within the covered entity. A disclosure of PHI means communicating that information to a person or entity outside the covered entity, or the communication of PHI from a health care component to a non-health care component of a hybrid entity. The Privacy Rule restricts both uses and disclosures of PHI, but it requires an accounting only for certain PHI disclosures.

Accounting of Disclosures – Information that describes a covered entity's disclosures of PHI other than for treatment, payment, and health care operations; disclosures made with Authorization; and certain other limited disclosures. For those categories of disclosures that need to be in the accounting, the accounting must include disclosures that have occurred during the 6 years (or a shorter time period at the request of the individual) prior to the date of the request for an accounting. However, PHI disclosures made before the compliance date for a covered entity are not part of the accounting requirement.

Use – With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the entity or health care component (for hybrid entities) that maintains such information.

Disclosure – The release, transfer, access to, or divulging of information in any other manner outside the entity holding the information.

Upon receiving an individual's request, a covered entity must account for disclosures of that individual's PHI made on or after the covered entity's compliance date (for most entities, April 14, 2003), unless a particular disclosure or type of disclosure is excluded from this accounting requirement in Section 164.528(a) of the Privacy Rule. For example, an accounting is not needed when the PHI disclosure is made:

- For treatment, payment, or health care operations.
- Under an Authorization for the disclosure.
- To an individual about himself or herself.
- As part of a limited data set under a data use agreement.
- Prior to the compliance date.

An individual's right to receive an accounting of disclosures (unless an exception applies) starts with the covered entity's compliance date and goes back 6 years from the date of the request, not including periods prior to the compliance date. A covered entity must therefore keep records of such PHI disclosures for 6 years.

The Privacy Rule allows three methods for accounting for research-related disclosures that are made without the individual's Authorization or other than a limited data set: (1) A standard approach, (2) a multiple-disclosures approach, and (3) an alternative for disclosures involving 50 or more individuals. Whatever approach is selected, the accounting is made in writing and provided to the requesting individual. Accounting reports to individuals may include results from more than one accounting method.

Standard Accounting

Standard accounting includes, for each disclosure, the following information:

- The date the disclosure was made.
- The name and, if known, address of the person or entity receiving the PHI.
- A brief description of the PHI disclosed.
- A brief statement of the reason for the disclosure.

Multiple Disclosures Accounting

Multiple disclosures accounting is permissible if the covered entity has made multiple disclosures of PHI to the same person or entity for a single purpose under Sections 164.502(a)(2)(ii) or 164.512 of the Privacy Rule. For each disclosure, the following must be included:

- The date the initial disclosure was made during the accounting period.
- The name and, if known, address of the person or entity receiving the PHI.
- A brief description of the PHI disclosed.

- A brief statement of the reason for the disclosure.
- The frequency, periodicity, or number of the disclosures made during the accounting period.
- The date of the last such disclosure during the accounting period.

Alternative Accounting

If a covered entity has made disclosures regarding 50 or more individuals for a particular research project under Section 164.512(i) of the Privacy Rule, the accounting may be limited to the following information:

- The name of the protocol or research activity.
- A plain-language description of the research protocol or activity, purpose of the research, and criteria for selecting particular records.
- A description of the type of PHI disclosed.
- The date or period of time during which the disclosure(s) occurred or may have occurred, including the date of the last disclosure during the accounting period.
- The name, address, and telephone number of the entity that sponsored the research and of the researcher who received the PHI.
- A statement that the individual's PHI may or may not have been disclosed for a particular protocol or research activity.

If the covered entity uses the alternative accounting method, it must, if requested to by the individual, assist the individual in contacting the research sponsor and the researcher. Such assistance, however, is limited to those situations in which there is a reasonable likelihood that the individual's PHI was actually disclosed for the research protocol or activity.

What Is the Effect of the Privacy Rule on Research Started Before the Compliance Date?

Key Point:

- Research that is ongoing before the applicable compliance date (usually April 14, 2003) is covered by the Privacy Rule's transition provisions if the research participant's informed consent, other legal permission for the research use and disclosure, or an IRB's waiver of informed consent was obtained by the covered entity before the applicable compliance date for the Privacy Rule.

The Privacy Rule includes a limited provision that "grandfathers" certain permissions obtained for research that were obtained prior to the compliance date. Under these transition provisions, a covered entity may use and disclose for the research purposes allowed by those permissions PHI that was created or received, either before or after the compliance date, if any one of the following is obtained before the compliance date:

- An Authorization or other express legal permission from an individual to use or disclose PHI for the research.
- The informed consent of the individual to participate in the research.
- A waiver of informed consent by an IRB.

Transition Provisions – A section of the Privacy Rule that permits covered entities to rely on express legal permission for use and disclosure of PHI, informed consent, or IRB-approved waiver of informed consent for research, provided the legal permission, informed consent, or IRB-approved waiver was obtained prior to the compliance date.

However, if a waiver of informed consent was obtained prior to the compliance date, but informed consent is sought from the research subject after the compliance date, the covered entity must obtain the individual's Authorization as required under the Privacy Rule unless such use or disclosure is permitted without Authorization. For example, if there had been a temporary waiver of informed consent for emergency research

under the FDA Protection of Human Subjects Regulations, and informed consent was later sought after the compliance date, a covered entity would have to obtain an individual Authorization before it could use or disclose PHI for the research, unless the activity is otherwise permitted by the Privacy Rule.

The Privacy Rule allows covered entities to rely on express legal permission, informed consent, or IRB-approved waiver of informed consent obtained before the compliance date to use and disclose PHI for research studies, as well as for any future research that may be included in such permission. This provision is different from those applying to an Authorization or a waiver obtained after the compliance date. Authorizations and waivers after the compliance date will only permit the use or disclosure for the specific research study for which they were obtained.

In some instances, existing express legal permissions, informed consents, or IRB-approved waivers of informed consents are not study specific. These permissions for research and waivers, even if provided for future unspecified research, are grandfathered by the transition provisions provided the permission or waiver was obtained prior to the compliance date and informed consent for research is not sought later.

Conclusion

The Privacy Rule introduces new standards for protecting the privacy of individuals' identifiable health information held by a covered entity or its business associates. For covered entities, the Privacy Rule sets minimum standards for how PHI may be used and disclosed and how individuals can have control of their health information, including for research purposes. For independent researchers who are not subject to the Privacy Rule, the Rule may affect access to such information.

The Privacy Rule was not intended to impede research. Rather, it provides ways to access vital information needed for research in a manner that protects the privacy of the research subject. The Privacy Rule describes methods to de-identify health information such that it is no longer PHI or governed by the Rule. If de-identified health information cannot be used for research, covered entities can obtain the individual's written permission for the research in an Authorization document describing the research uses and disclosures of PHI and the rights of the research subject. When obtaining the Authorization form is not practicable, an IRB or Privacy Board could waive or alter the Authorization requirement. The Privacy Rule also provides alternatives to obtaining an Authorization or a waiver or an alteration of this requirement, such as limited data sets or with representations provided for certain research activities. The Privacy Rule also contains a provision that "grandfathers" research that is ongoing before the compliance date to facilitate compliance with the Rule.

Many researchers are accustomed to complying with Federal and State regulations that protect participants from research risks; some of these regulations even require, as applicable, a researcher to describe privacy and confidentiality protections in an informed consent. While the Privacy Rule may add to these privacy protections, researchers are aware of the importance of protecting research subjects from foreseeable research risks, including risks to privacy. Understanding how and why the Privacy Rule protects the privacy of identifiable health information is an important step in understanding how covered entities implement the Rule's standards.

Because the Privacy Rule is new and introduces new standards for how PHI is handled by covered entities, researchers and their institutions may have questions about the Rule. Researchers are encouraged to contact their institution, IRB, counsel, or Privacy Officer to learn more about how the Privacy Rule affects their institution. Questions and comments about the Privacy Rule may also be sent to HHS's Office for Civil Rights (OCR) at ocrprivacy@hhs.gov. Several other Federal agencies are also prepared to assist researchers with questions about the Privacy Rule. Information can be found at the sites listed on the next page.

Sources of Information About the Privacy Rule

HIPAA Privacy Rule

- **The final HIPAA Privacy Rule is available at** http://www.hhs.gov/ocr/hipaa**.**

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.ahrq.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
- **National Institutes of Health (NIH)**
  http://privacyruleandresearch.nih.gov/
- **Office for Human Research Protections (OHRP), HHS**
  http://ohrp.osophs.dhhs.gov/
- **Substance Abuse and Mental Health Services Administration (SAMHSA)**
  http://www.hipaa.samhsa.gov/

Glossary

The terms and definitions defined or described here have been summarized from the Privacy Rule. Refer to the Privacy Rule for a complete listing of terms and their specific definitions.

***Accounting for Disclosures* – Information that describes a covered entity's disclosures of PHI other than for treatment, payment, and health care operations; disclosures made with Authorization; and certain other limited disclosures. For those categories of disclosures that need to be in the accounting, the accounting must include disclosures that have occurred during the 6 years (or a shorter time period at the request of the individual) prior to the date of the request for an accounting. However, PHI disclosures made before the compliance date for a covered entity are not part of the accounting requirement.**

***Authorization* – An individual's written permission to allow a covered entity to use or disclose specified PHI for a particular purpose. Except as otherwise permitted by the Rule, a covered entity may not use or disclose PHI for research purposes without a valid Authorization.**

***Business Associate* – A person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, or any other function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule. Business associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of individually identifiable health information by the covered entity or another business associate of the covered entity to that person or entity. A member of a covered entity's workforce is not one of its business associates. A covered entity may be a business associate of another covered entity.**

***Compliance Date* – The date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under the Privacy Rule. With the exception of small health plans, which have an extra year to comply, covered entities must complete implementation of, and be in compliance with, the Privacy Rule by April 14, 2003.**

***Covered Entity* – A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard.**

***Covered Functions* – Those functions of a covered entity the performance of which makes the entity a health care provider, health plan, or health care clearinghouse under the HIPAA Administrative Simplification Rules.**

***Data Use Agreement*– An agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.**

***Designated Record Set* – A group of records maintained by or for a covered entity that includes (1) medical and billing records about individuals maintained by or for a covered health care provider; (2) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for the covered entity to make decisions about individuals. A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.**

Disclosure **– The release, transfer, access to, or divulging of information in any other manner outside the entity holding the information.**

FDA Protection of Human Subjects Regulations **– Regulations intended to protect the rights, safety, and welfare of participants involved in studies subject to FDA jurisdiction. The FDA Protection of Human Subjects Regulations can be found at Title 21 *Code of Federal Regulations*, Parts 50 and 56.**

Health Care **– Care, services, or supplies related to the health of an individual, including (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.**

Health Care Clearinghouse **– A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches that either process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or receive a standard transaction from another entity and process or facilitate the processing of health information into a nonstandard format or nonstandard data content for the receiving entity.**

Health Care Provider **– A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.**

Health Information **– Any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.**

Health Insurance Portability and Accountability Act of 1996 (HIPAA) **– This Act requires, among other things, under the Administrative Simplification subtitle, the adoption of standards, including standards for protecting the privacy of individually identifiable health information.**

Health Plan **– For the purposes of Title II of HIPAA, an individual or group plan that provides or pays the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)) and including entities and government programs listed in the Rule. Health plan excludes: (1) any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and (2) a government-funded program (unless otherwise included at section 160.103 of HIPAA) whose principal purpose is other than providing, or paying for the cost of, health care or whose principal activity is the direct provision of health care to persons or the making of grants to fund the direct provision of health care to persons.**

HHS Protection of Human Subjects Regulations **– Regulations intended to protect the rights and welfare of human subjects involved in research conducted or supported by HHS. The HHS regulations include the Federal Policy for the Protection of Human Subjects, effective August 19, 1991, and provide additional protections for pregnant women, fetuses, neonates, prisoners, and children involved in research. The HHS regulations can be found at Title 45 of the *Code of Federal Regulations,* Part 46.**

***Hybrid Entity* – A single legal entity that is a covered entity, performs business activities that include both covered and noncovered functions, and designates its health care components as provided in the Privacy Rule. If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components. However, non-health care components of a hybrid entity may be business associates of one or more of its health care components, depending on the nature of their relationship.**

***Individually Identifiable Health Information* – Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.**

***Institutional Review Board (IRB)* – An IRB can be used to review and approve a researcher's request to waive or alter the Privacy Rule's requirements for an Authorization. The Privacy Rule does not alter the membership, functions and operations, and review and approval procedures of an IRB regarding the protection of human subjects established by other Federal requirements.**

***Limited Data Set* – Refers to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's Authorization or a waiver or an alteration of Authorization for its use and disclosure, with a data use agreement.**

***Minimum Necessary* – The least information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request. Unless an exception applies, this standard applies to a covered entity when using or disclosing PHI or when requesting PHI from another covered entity. A covered entity that is using or disclosing PHI for research without Authorization must make reasonable efforts to limit PHI to the minimum necessary. A covered entity may rely, if reasonable under the circumstances, on documentation of IRB or Privacy Board approval or other appropriate representations and documentation under section 164.512(i) as establishing that the request for protected health information for the research meets the minimum necessary requirements.**

***Privacy Board* – A board that is established to review and approve requests for waivers or alterations of Authorization in connection with a use or disclosure of PHI as an alternative to obtaining such waivers or alterations from an IRB. A Privacy Board consists of members with varying backgrounds and appropriate professional competencies as necessary to review the effect of the research protocol on an individual's privacy rights and related interests. The board must include at least one member who is not affiliated with the covered entity, is not affiliated with any entity conducting or sponsoring the research, and is not related to any person who is affiliated with any such entities. A Privacy Board cannot have any member participating in a review of any project in which the member has a conflict of interest.**

***Protected Health Information* – PHI is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.**

Research **– A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of research repositories and databases for research.**

State Law **– A constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.**

Transaction **– The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:**

1. **Health care claims or equivalent encounter information.**
2. **Health care payment and remittance advice.**
3. **Coordination of benefits.**
4. **Health care claim status.**
5. **Enrollment and disenrollment in a health plan.**
6. **Eligibility for a health plan.**
7. **Health-plan premium payments.**
8. **Referral certification and authorization.**
9. **The HHS Secretary is also required to adopt standards for first report of injury, claims attachments, and other transactions that the HHS Secretary may prescribe by regulation.**

Transition Provisions **– A section of the Privacy Rule that permits covered entities to rely on express legal permission for use and disclosure of PHI, informed consent, or IRB-approved waiver of informed consent for research, provided the legal permission, informed consent, or IRB-approved waiver was obtained prior to the compliance date.**

Use **– With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the entity or health care component (for hybrid entities) that maintains such information.**

Waiver or Alteration of Authorization **– The documentation that the covered entity obtains from a researcher or an IRB or a Privacy Board that states that the IRB or Privacy Board has waived or altered the Privacy Rule's requirement that an individual must authorize a covered entity to use or disclose the individual's PHI for research purposes.**

Workforce **– Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of the covered entity, whether or not they are paid by the covered entity.**

Index

NIH Publication Number 03-5388

Research Repositories, Databases, and the HIPAA Privacy Rule

Overview

Researchers in medical and health-related disciplines require access to many sources of health information, from archived medical records and epidemiological databases to disease registries, tissue repositories, hospital discharge records, and government compilations of vital and health records. As the Privacy Rule is implemented, researchers are asking how these rules might affect research that uses records within databases and repositories.

As of April 14, 2003, the Privacy Rule requires many health care providers and health insurers to obtain additional documentation from researchers before disclosing health information to them, and to scrutinize researchers' requests for access to health information more closely. Although the Privacy Rule introduces new rules for the use and disclosure of health information by covered entities for research, researchers can help to enable their continued access to health data by understanding the Privacy Rule and assisting health care entities covered by the Privacy Rule in meeting its requirements.

This fact sheet discusses the Privacy Rule and its potential to affect the creation of research databases and repositories, and research that uses identifiable health information in repositories and databases. Additional information about the Privacy Rule's potential impact on other research activities, such as clinical research, health services research, institutional review boards (IRBs) and Privacy Boards can be found in related publications, including:

- *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*
- *Health Services Research and the HIPAA Privacy Rule*
- *Clinical Research and the HIPAA Privacy Rule*
- *Institutional Review Boards and the HIPAA Privacy Rule*
- *Privacy Boards and the HIPAA Privacy Rule*

Introduction to the Privacy Rule

In response to a congressional mandate in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services (HHS) issued regulations entitled, *Standards for Privacy of Individually Identifiable Health Information*. For most covered entities, compliance with these regulations, known as the Privacy Rule, was required as of April 14, 2003.

The Privacy Rule is a response to public concern over potential abuses of the privacy of health information. The Privacy Rule establishes a category of health information, referred to as protected health information (PHI), which may be used or disclosed to others only in certain circumstances or under certain conditions. PHI is a subset of what is termed *individually identifiable health information*. With certain exceptions, the Privacy Rule applies to individually identifiable health information created or maintained by a covered entity. Covered entities are health plans, health care clearinghouses, and health care providers that transmit health information electronically in connection with certain defined HIPAA transactions, such as claims or eligibility inquiries. Researchers are not themselves covered entities, unless they are also health care providers and engage in any of the covered electronic transactions. If, however, researchers are employees or other workforce members of a covered entity (e.g., a covered hospital or health insurer), they may have to comply with that entity's HIPAA privacy policies and procedures. Researchers who are not themselves covered entities, or who are not workforce members of covered entities, may be indirectly affected by the Privacy Rule if covered entities supply their data. The HHS and the Food and Drug Administration's (FDA) Protection of Human Subjects Regulations (45 CFR part 46 and 21 CFR parts 50 and 56, respectively) may also apply to research involving the development or use of research repositories and associated data.

Overview of the Privacy Rule's Impact on Repositories and Databases

The Privacy Rule was not intended to impede research using records within databases and repositories that include individuals' health information, but the Privacy Rule does place new conditions on the use and disclosure of PHI by covered entities for research. The creation of a research database or repository, and the use or disclosure of PHI from a database or repository for research, may each be considered a research activity under the Privacy Rule. For more specific information about how the Privacy Rule could affect health services research, refer to the related publication, *Health Services Research and the HIPAA Privacy Rule*.

It is important to know that the Privacy Rule permits covered entities, such as hospitals, clinics, and other health care providers to continue amassing information on their patients for treatment, payment, and health care operations purposes, and to enter this information into their own databases without Authorization. The Privacy Rule also allows the disclosure of PHI to government-authorized public health authorities for disease surveillance, disease prevention, and other public health purposes, such as reporting disease and injury. When required by law, other disclosures are permitted, for example, state-mandated reporting to cancer registries. Covered entities may also continue to disclose PHI for adverse event and related reports to FDA and others for public health purposes (see section 164.512 of the Privacy Rule and additional information at *http://www.cdc.gov/mmwr/early_release.html*). Thus, many databases that are now used for records research continue to be maintained and updated, and will remain available to records researchers, although in some cases, under new terms.

The Privacy Rule permits a covered entity to use or disclose PHI for research under the following circumstances and conditions:

- For reviews preparatory to research if certain representations are obtained from the researcher
- For research solely on decedents' information if certain representations are obtained from the researcher
- If the subject of the PHI has granted specific written permission through an Authorization
- If the covered entity receives appropriate documentation that an IRB or Privacy Board has granted a waiver or an alteration of the Authorization requirement
- If the PHI has been de-identified in accordance with the standards set by the Privacy Rule (in which case, the health information is no longer PHI)
- If the information is released in the form of a limited data set, with certain identifiers removed, and with a data use agreement between the researcher and the covered entity
- If informed consent of the individual to participate in the research, an IRB waiver of such informed consent, or other express legal permission to use or disclose the information for the research is grandfathered by the transition provisions

For some records and database research, Authorization may not be needed. Some of the most important exceptions to the Authorization requirement that pertain to research using repositories and databases are the waiver of Authorization and the limited data set.

Waiver or Alteration of the Authorization Requirement by an IRB or Privacy Board

For some types of research, it may be impracticable for researchers to obtain written Authorization from research participants, for example, for some research conducted on existing databases or repositories where no contact information is available. To address these situations, the Privacy Rule contains criteria for the waiver or alteration of the Authorization requirement by an IRB or another review body called a Privacy Board. The Privacy Rule permits a covered entity to use or disclose PHI for research purposes without Authorization (or with an altered Authorization), if the covered entity received proper documentation that an IRB or Privacy Board has granted a waiver (or an alteration) of the Authorization

requirement for the research use or disclosure of PHI. The Privacy Rule establishes criteria to be evaluated by an IRB or Privacy Board in approving an Authorization waiver or alteration. For a covered entity to use or disclose PHI under a waiver or alteration of the Authorization requirement, it must receive documentation of, among other things, the IRB or Privacy Board's determination that the following criteria have been met:

- The PHI use or disclosure involves no more than a minimal risk to the privacy of individuals based on at least the presence of (1) An adequate plan presented to the IRB or Privacy Board to protect PHI identifiers from improper use and disclosure; (2) an adequate plan to destroy those identifiers at the earliest opportunity, consistent with the research, absent a health or research justification for retaining the identifiers or if retention is otherwise required by law; and (3) adequate written assurances that the PHI will not be reused or disclosed to any other person or entity except (a) as required by law, (b) for authorized oversight of the research study, or (c) for other research for which the use or disclosure of the PHI is permitted by the Privacy Rule.
- The research could not practicably be conducted without the requested waiver or alteration.
- The research could not practicably be conducted without access to and use of the PHI.

Additional information about waivers and alterations of Authorization can be found in the publications: *Institutional Review Boards and the HIPAA Privacy Rule* and *Privacy Boards and the HIPAA Privacy Rule*.

De-identified Data Sets

The Privacy Rule permits covered entities to release data that have been de-identified without obtaining an Authorization and without further restrictions upon use or disclosure because de-identified data is not PHI and, therefore, not subject to the Privacy Rule. A covered entity may de-identify PHI in one of two ways. The first way, the "safe-harbor" method, is to remove all 18 identifiers enumerated at section 164.514(b)(2) of the regulations.[1] Data that are stripped of these 18 identifiers are regarded as de-identified, unless the covered entity has actual knowledge that it would be possible to use the remaining information alone or in combination with other information to identify the subject.

The second way is to have a qualified statistician[2] determine, using generally accepted statistical and scientific principles and methods, that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by the anticipated recipient to identify the subject of the information. The qualified statistician must document the methods and results of the analysis that justify such a determination.

It is important to know that the Privacy Rule permits a covered entity to assign to, and retain with, the de-identified health information, a code or other means of record re-identification if that code is not derived from or related to the information about the individual and is not otherwise capable of being translated to identify the individual. For example, an encrypted individual identifier (e.g., a social security number) would not meet the conditions for use as a re-identification code for de-identified health information because it is derived from individually identified information. (See 67 *Federal Register* 53233, August 14, 2002.) In addition, the covered entity may not (1) use or disclose the code or other means of record identification for any purposes other than as a re-identification code for the de-identified data, and (2) disclose its method of re-identifying the information.

Limited Data Sets

Where only certain identifiers are needed, it may be permissible for a covered entity to provide a researcher with a limited data set. Limited data sets are data sets stripped of certain direct identifiers that are specified in the Privacy Rule. Limited data sets may be used or disclosed only for public health, research, or health care operations purposes. They are not de-identified information under the Privacy Rule. Importantly, unlike de-identified data, protected health information in limited data sets may include the following: Addresses other than street name or street address

or post office boxes, all elements of dates (such as admission and discharge dates) and unique codes or identifiers not listed as direct identifiers.[3]

Before disclosing a limited data set to a researcher, a covered entity must enter into a data use agreement with the researcher, identifying the researcher as the recipient of the limited data set, establishing how the data may be used and disclosed by the recipient, and providing assurances that the data will be protected, among other requirements. If the covered entity learns that the researcher has violated this agreement, the entity must take reasonable steps to end or repair the violation and, if such steps are unsuccessful, stop disclosing PHI to the researcher and report the problem to the HHS Office for Civil Rights. Additional information on limited data sets and data use agreements can be found in the booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*.

Activities Preparatory to Research

Covered entities may permit researchers to review PHI in medical records or elsewhere to prepare a research protocol, or for similar purposes preparatory to research. This review allows the researcher to determine, for example, whether a sufficient number or type of records exists to conduct the research. Importantly, the covered entity may not permit the researcher to remove any PHI from the covered entity. To permit the researcher to conduct a review preparatory to research, the covered entity must receive from the researcher representations that:

- The use or disclosure is sought solely to review PHI as necessary to prepare the research protocol or other similar preparatory purposes.
- No PHI will be removed from the covered entity during the review.
- The PHI the researcher seeks to use or access is necessary for the research purposes.

Additional information on activities preparatory to research can be found in the publications, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule* and *Clinical Research and the HIPAA Privacy Rule*.

Research Involving Decedents' PHI

A covered entity may provide access to decedents' records for research purposes if the covered entity receives from the researcher: Representations that the decedents' PHI is necessary for the research and is being sought solely for research on the PHI of decedents (not, for example, living relatives of decedents); and, upon request of the covered entity, documentation of the deaths of the study subjects. No Authorization or alteration or waiver of Authorization by an IRB or Privacy Board is needed for use or disclosure of PHI for research only on the PHI of deceased persons, if these conditions are met.

Other Privacy Rule Requirements

Minimum Necessary Standard

When using or disclosing PHI for research without an Authorization, a covered entity must make reasonable efforts to limit the PHI used or disclosed to the minimum necessary amount to accomplish the research purpose. If an IRB or Privacy Board has granted the researcher a waiver or an alteration of Authorization, a covered entity may reasonably rely upon the researcher's request consistent with the description of PHI in documentation from the IRB or Privacy Board as the minimum necessary amount of PHI for the research. Additional information on the minimum necessary standard can be found in the booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*.

Right to an Accounting of Disclosures

The Privacy Rule grants individuals new rights, including the right to receive an accounting of disclosures made for research by a covered entity without the individual's Authorization (e.g., under a waiver of Authorization), except for disclosures of a limited data set. The individual has a right to such an accounting of disclosures made by a covered entity in the 6 years prior to the date on which the accounting is requested, not including the period prior to the compliance date. For such

disclosures, in general, individuals who request an accounting must be told what PHI was disclosed, to whom it was disclosed, and the date and purpose of the disclosure. Covered entities must provide the address of the recipient, if known.

For certain research disclosures made by a covered entity, two other options exist for providing an accounting. When multiple disclosures of PHI are made to the same person or entity for a single purpose, the accounting for such disclosures may consist of the information described above for the first disclosure, plus the number or frequency of disclosures, and the date of the last disclosure during the time period covered by the request.

If, during the period covered by the accounting, the covered entity has disclosed the records of 50 or more individuals for a particular research purpose, the covered entity may provide a more general accounting to the requestor. The covered entity would provide the following information in the general accounting:

- The name and description of the protocols for which their PHI may have been disclosed
- A brief description of the type of PHI disclosed
- The date or period of time of the disclosures
- The contact information of the researcher and the research sponsor
- A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or research activity

Section 164.528(b)(4)(ii) of the Privacy Rule requires that, upon request, the covered entity must help the individual contact the sponsor and researcher when it is reasonably likely that the individual's PHI was disclosed for a particular protocol. Additional information on accounting of disclosures can be found in the booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*.

Frequently Asked Questions and Answers

Q: Are tissue repositories covered entities?

A: Not unless the organization maintaining the tissue repository conducts some other activity that makes it a covered entity. For example, tissue repositories that conduct testing of specimens for the benefit of transplant recipients based on another health care provider's orders would be covered providers under HIPAA if they conduct electronic transactions for which the HHS has adopted standards.

Q: A researcher does not receive names, addresses, social security or medical record numbers, or other obvious identifiers from data sources. If the IRB has not considered this data to be individually identifiable in the past, and thus, determined that the research was not human subjects research under 45 CFR part 46, or that the research was exempt under 45 CFR 46.101(b), will this change under the Privacy Rule?

A: No. The Privacy Rule does not change the applicability or the requirements of the HHS and FDA Protection of Human Subjects Regulations. However, where the information sought by the researcher is held by a covered entity, the covered entity's use or disclosure of that information is subject to the Privacy Rule, unless the information is de-identified by the Privacy Rule's standards. The Privacy Rule's de-identification safe-harbor method is likely more stringent than what has been applied in the past to render information no longer identifiable for research purposes. De-identification under the Privacy Rule's safe-harbor standard may be accomplished through the removal of all 18 identifiers (section 164.514(b)(2) of the Privacy Rule).

Alternatively, fewer identifiers may need to be removed for health information to be de-identified if a qualified statistician determines that the risk of re-identification is very small (section 164.514(b)(1) of the Privacy Rule).

The Privacy Rule also permits a covered entity to retain, with the de-identified health information, a code for re-identification as long as the code is not related to or derived from information about the individual and is not otherwise capable of being translated to identify the individual, and as long as the covered entity does not disclose its method of re-identification or use or disclose its code for other purposes (section 164.514(c) of the Privacy Rule). For example, a randomly assigned re-identification code would not make the de-identified information to which it is assigned PHI, because a random code would not be derived from or related to information about the individual.

Where a researcher needs data elements that would render the information identifiable under the Privacy Rule, but where certain direct identifiers (set forth in section 164.514(e)) are not needed, a limited data set may be sufficient for the research. A limited data set is information stripped of only the direct identifiers listed at section 164.514(e), which include, but are not limited to, the name and street address of the individual. To use or disclose a limited data set, the covered entity must enter into a data use agreement with the recipient of the information.

In practice, this means that records research that may not require IRB approval under the HHS Protection of Human Subjects Regulations, still may require an Authorization or a waiver of Authorization under the Privacy Rule, or be subject to a data use agreement if a limited data set is used or disclosed.

Q: How may a covered entity use or disclose PHI for the creation of a research repository or database when it is unknown at the time of collection what specific protocols will make use of the repository or database in the future?

A: There are two separate activities to consider: (1) The use or disclosure of PHI for creating a research database or repository and (2) The subsequent use or disclosure of PHI in the database for a particular research protocol.

A covered entity's use or disclosure of PHI to create a research database or repository, and use or disclosure of PHI from the database or repository for a future research purpose, are each considered a separate research activity under the Privacy Rule. In general, the Privacy Rule requires Authorization for each activity, unless, for example, an IRB or Privacy Board waives or alters the Authorization requirement. (See **Overview of Privacy Rule's Impact on Repositories and Databases**.) Documentation of a waiver or an alteration of Authorization to use or disclose PHI to create a research database requires, among other things, a statement that an IRB or Privacy Board has determined that the researcher has provided adequate written assurances that PHI in the database will not be further used or disclosed except as permitted by the Privacy Rule (e.g., for research uses and disclosures with an Authorization or waiver). A covered entity also could use or disclose a limited data set to create a research repository or database under conditions set forth in a data use agreement.

For subsequent use or disclosure of PHI for research purposes from a repository or database maintained by the covered entity, the covered entity may:

- Obtain the individual's Authorization for the research use or disclosure of PHI as specified under section 164.508
- Obtain documentation of an IRB or Privacy Board's waiver of the Authorization requirement that satisfies section 164.512(i)
- Obtain satisfactory documentation of an IRB or Privacy Board's alteration of the Authorization requirement as well as the altered Authorization from the individual
- Use or disclose PHI for reviews preparatory to research with representations that satisfy

section 164.512(i)(1)(ii) of the Privacy Rule
- Use or disclose PHI for research on decedents' PHI with representations that satisfy section 164.512(i)(1)(iii) of the Privacy Rule
- Provide a limited data set and enter into a data use agreement with the recipient as specified under section 164.514(e)
- Use or disclose PHI based on permission obtained prior to the compliance date of the Privacy Rule—informed consent of the individual to participate in the research, an IRB waiver of such informed consent, or Authorization or other express legal permission to use or disclose the information for the research as specified under section 164.532(c) of the Privacy Rule

A covered entity may also use or disclose PHI from databases and repositories for other purposes without Authorization as permitted by the Privacy Rule, such as if required by law or to a public health authority for a public health activity (e.g., disclosures to cancer registries). Covered entities may also de-identify PHI according to standards set forth in the Privacy Rule so that its use and disclosure are not protected by the Privacy Rule.

Q: May a single Authorization permit a covered entity to use or disclose PHI for multiple activities of a specific research study, including the collection and storage of tissues for only that study? Does the option for using a single Authorization differ if a research study also collects and stores PHI as part of a central repository for future research?

A: A single Authorization may cover uses and disclosures of PHI for multiple activities of a specific research study, including the collection and storage of tissues for that study. In addition, where two different research studies are involved, such as where a research study collects information for the study itself, and collects and stores PHI in a central repository for future research, the Privacy Rule generally would permit them to be combined into a single, compound Authorization form.

However, a compound Authorization is not allowed where the provision of research-related treatment, payment, or eligibility for benefits is conditioned on only one of the Authorizations, and not the other. See section 164.508(b)(3)(iii) of the Privacy Rule. For example, a covered entity that conducts an interventional clinical trial that also involves collecting tissues and associated PHI for storage in a central repository for future research would not be permitted to obtain a compound Authorization for both research purposes if research-related treatment is conditioned upon signing the Authorization for the clinical trial. Any compound Authorization must clearly specify the different research studies covered by the Authorization so the individual is adequately informed.

Q: How could the Privacy Rule affect research involving data from repositories or databases that were created prior to the Privacy Rule's compliance date (April 14, 2003)?

A: The Privacy Rule contains a transition provision that, under certain conditions, allows covered entities to continue to use or disclose PHI without an Authorization, or waiver or alteration of the Authorization requirement, in connection with ongoing research, including research involving repositories or databases. For many such uses and disclosures of PHI in connection with ongoing research, a covered entity may rely on any one of the following that was obtained prior to the compliance date:

- An Authorization or other express legal permission from an individual to use or disclose PHI for research
- The informed consent of the individual to participate in the research
- A waiver by an IRB of informed consent in accordance with applicable laws and regulations governing informed consent, unless informed consent is sought after the compliance date

If the transition provisions do not apply and the information is not de-identified, subse-

quent uses and disclosures of PHI from databases and repositories held by covered entities generally require an individual's Authorization unless otherwise permitted by the Privacy Rule (e.g., with a waiver of Authorization or as a limited data set).

In addition, if the database or repository, which is held or maintained by a covered entity, contains only de-identified health information (which may include a re-identification code) meeting the Privacy Rule's requirements at section 164.514(a)-(c), the Privacy Rule does not apply.

Q: Does the Privacy Rule apply if a covered entity maintains and conducts research on a database of pre-existing specimens and data that are considered exempt from the HHS Protection of Human Subjects Regulations?

A. Yes, if the database contains PHI, the Privacy Rule applies. The covered entity, however, may de-identify the data by either: (1) Removing the 18 identifiable data elements listed at section 164.514(b)(2) of the Privacy Rule and having no actual knowledge that the information could be used, alone or in combination with other information, to identify the subject; or (2) having a qualified statistician's certification, with appropriate documentation, that there is a very small risk of identification by an anticipated recipient. If the information is not de-identified, subsequent uses and disclosures of PHI from databases and repositories held by covered entities generally require an individual's Authorization unless otherwise permitted by the Privacy Rule (e.g., with a waiver of Authorization or as a limited data set).

Q: A covered entity has a research repository and database of individually identifiable data for which the IRB waived informed consent for its creation and subsequent uses and disclosures of identifiable data prior to April 14, 2003. Is the covered entity required to obtain Authorization for research use and disclosure of PHI from the repository or database after April 14, 2003?

A: No, because the waiver, as described, meets the transition provisions of the Privacy Rule at 164.532(c). However, if informed consent is being sought from specimen donors after the compliance date, Authorization by the donors will be needed unless an IRB approves a waiver of the Authorization requirement, or another permitted use or disclosure applies.

Q: Does the Privacy Rule apply to databases held by covered entities that only receive de-identified participant data?

A: No, so long as the health information is de-identified according to the Privacy Rule, the Privacy Rule does not apply to the database or to future uses and disclosures of de-identified data from the database.

Q: May ongoing longitudinal studies continue after April 14, 2003?

A: Yes. Permissions or waivers obtained prior to the Privacy Rule's compliance date of April 14, 2003, for ongoing longitudinal studies are grandfathered by the Privacy Rule if they meet the transition provisions at 164.532(c). For many such uses and disclosures of PHI in connection with ongoing research, a covered entity may rely on any one of the following that was obtained prior to the compliance date:

- An Authorization or other express legal permission from an individual to use or disclose PHI for research
- The informed consent of the individual to participate in the research
- A waiver by an IRB of informed consent in accordance with applicable laws and regulations governing informed consent, unless informed consent is sought after the compliance date

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

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

Q: Does the Privacy Rule permit a covered entity to de-identify health information or create a limited data set without obtaining Authorization, waiver of the Authorization requirement from an IRB or Privacy Board, or representations for reviews preparatory to research?

A: Yes. In the Privacy Rule, creating de-identified health information or a limited data set is a health care operation of the covered entity, and thus, does not require the covered entity to obtain an individual's Authorization, a waiver of the Authorization requirement, or representations for reviews preparatory to research. If a business associate is hired by a covered entity to de-identify health information or create a limited data set, such activity must be conducted in accordance with the business associate requirements at sections 164.502(e) and 164.504(e).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A: The Privacy Rule provides individuals special protection for psychotherapy notes, which are notes recorded by a mental health provider that document or analyze counseling session conversations, and are maintained separately from the medical record. Unless the covered provider obtained, prior to the compliance date, the individual's informed consent or other express legal permission for the research or an IRB waiver of informed consent for the research, a covered entity may not use or disclose these notes for research without the individual's written Authorization. Information in the medical record and certain types of information, even if maintained separately from the medical record (e.g., information about test results, length and frequency of treatment, diagnosis, symptoms, or progress), is excluded from the definition of psychotherapy notes and may be released to researchers who obtain an Authorization or a waiver of Authorization from an IRB or Privacy Board, as part of a limited data set, or if appropriate, for reviews preparatory to research or for research involving decedent's information where required representations are obtained. Special requirements also apply to compound authorizations involving the use or disclosure of psychotherapy notes. (See section 164.508(b)(3)(ii) of the Privacy Rule.) Various state laws governing the use or disclosure of mental health records, including psychotherapy notes, which are more stringent than the Privacy Rule provisions, may also apply.

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

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

Q: Do the transition provisions apply to a surgical consent obtained by a covered provider that was signed or agreed to prior to the removal of tissues that were later added to a repository?

A: Yes, the transition provisions would apply in this case if, in the surgical consent or other express legal permission, the individual specifically agreed to the use and disclosure of PHI for research.

Q: Do the transition provisions at section 164.532(c) of the Privacy Rule apply to informed consent or waiver of informed consent to store and use PHI in a repository or database that was obtained before the compliance date?

A: Yes. HHS has stated, "…some express legal permissions and informed consents have not been study-specific and sometimes authorize the use or disclosure of information for future unspecified research. Furthermore, some IRB-approved waivers of informed consent have been for future unspecified research. Therefore, the final Rule at [section] 164.532 permits covered entities to rely on an express legal permission, informed consent, or IRB-approved waiver of informed consent for future unspecified research, provided the legal permission, informed consent or IRB-approved waiver was obtained prior to the compliance date." (See 67 *Federal Register* 53226, August 14, 2002.)

Q: Does the Privacy Rule limit, to specific types of research studies, disclosures permitted as preparatory to research or for research on decedents' information?

A: No. The Privacy Rule does not limit the types of research studies that may rely upon the provisions for reviews preparatory to research or for research on decedents' information set forth at section 164.512(i). However, representations made to satisfy these provisions must include, among other requirements at sections 164.512(i)(1)(ii) and 164.512(i)(1)(iii), a statement that the use or disclosure of protected health information is "necessary for the research purposes."

Q: Does the Privacy Rule restrict access for research purposes to information held by the Medicaid or SCHIP programs?

A: Yes. Local and state Medicaid authorities are covered entities under HIPAA, as are the State Children's Health Insurance Program (SCHIP) programs. These agencies or programs are covered under the Privacy Rule because they are listed in the Privacy Rule's definition of a "health plan." All SCHIP programs and state Medicaid agencies must consequently comply with the Privacy Rule; if they are hybrid entities, they must ensure that their designated health care components comply with the Privacy Rule. These government units will have some mechanism (a privacy officer, a Privacy Board, and/or an IRB) for controlling access to PHI for research purposes. A researcher will need to identify the responsible party and discuss with that office or official the ways in which access to PHI may be granted for research.

Q: In conducting records research, will a researcher who is a covered entity still be required to comply with state laws relating to medical records privacy, such as state HIV/AIDS confidentiality laws?

A: Probably. If the state law does not conflict with the Privacy Rule, the state law is not preempted by HIPAA, and the covered entity will be required to comply with both the state law and the Privacy Rule. If the state law conflicts with a provision of the Privacy Rule, the Privacy Rule has a preemption provision that allows state medical privacy laws to remain in place, if they are more stringent than the federal privacy standards. The Privacy Rule does not prohibit states from adopting privacy protections that are more stringent than the federal privacy standards.

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

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

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

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

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

[1] The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed: (1) Names; (2) all geographic subdivisions smaller than a state, except for the initial three digits of the ZIP code if the geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; (3) all elements of dates except year, and all ages over 89 or elements indicative of such age; (4) telephone numbers; (5) fax numbers; (6) email addresses; (7) social security numbers; (8) medical record numbers; (9) health plan beneficiary numbers; (10) account numbers; (11) certificate or license numbers; (12) vehicle identifiers and license plate numbers; (13) device identifiers and serial numbers; (14) URLs; (15) IP addresses; (16) biometric identifiers; (17) full-face photographs and any comparable images; (18) any other unique, identifying characteristic or code, except as permitted for re-identification in the Privacy Rule.

[2] A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.

[3] The following direct identifiers must be removed for PHI to qualify as a limited data set: (1) Names; (2) postal address information, other than town or city, state, and ZIP code; (3) telephone numbers; (4) fax numbers; (5) email addresses; (6) social security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate or license numbers; (11) vehicle identifiers and license plate numbers; (12) device identifiers and serial numbers; (13) URLs; (14) IP addresses; (15) biometric identifiers; and (16) full-face photographs and any comparable images.

NIH Publication Number 04-5489 January 2004

HIPAA Authorization for Research

Overview

A Privacy Rule Authorization is an individual's signed permission to allow a covered entity to use or disclose the individual's protected health information (PHI) that is described in the Authorization for the purpose(s) and to the recipient(s) stated in the Authorization. In contrast, an informed consent document is an individual's agreement to participate in the research study and includes a description of the study, anticipated risks and/or benefits, and how the confidentiality of records will be protected, among other things. An Authorization can be combined with an informed consent document or other permission to participate in research. If a covered entity obtains or receives a valid Authorization for its use or disclosure of PHI for research, it may use or disclose the PHI for the research, but the use or disclosure must be consistent with the Authorization.

The Authorization must be written in plain language. A copy of the signed Authorization must be provided to the individual signing it if the covered entity itself is seeking the Authorization. The Privacy Rule does not specify who must draft the Authorization, so a researcher could draft one. The Privacy Rule specifies core elements and required statements that must be included in an Authorization. An Authorization is not valid unless it contains all the required elements and statements. An Authorization form may also, but is not required to, include additional, optional elements so long as they are not inconsistent with the required elements and statements and are not otherwise contrary to the Authorization requirements of the Privacy Rule. An Authorization, whether prepared by a covered entity or by a person requesting PHI from a covered entity, must include the following core elements and required statements:

Authorization Core Elements (see Privacy Rule, *45 C.F.R.* §164.508(c)(1))

- Description of PHI to be used or disclosed (identifying the information in a specific and meaningful manner).
- The name(s) or other specific identification of person(s) or class of persons authorized to make the requested use or disclosure.
- The name(s) or other specific identification of the person(s) or class of persons who may use the PHI or to whom the covered entity may make the requested disclosure.
- Description of each purpose of the requested use or disclosure. Researchers should note that this element must be research study specific, not for future unspecified research.
- Authorization expiration date or event that relates to the individual or to the purpose of the use or disclosure (the terms "end of the research study" or "none" may be used for research, including for the creation and maintenance of a research database or repository).
- Signature of the individual and date. If the Authorization is signed by an individual's personal representative, a description of the representative's authority to act for the individual.

Authorization Required Statements (see Privacy Rule, *45 C.F.R.* § 164.508(c)(2))

- The individual's right to revoke Authorization in writing and either (1) the exceptions to the right to revoke and a description of how the individual may revoke Authorization or (2) reference to the corresponding section(s) of the covered entity's Notice of Privacy Practices.
- Notice of the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the Authorization, including research-related treatment, and, if applicable, consequences of refusing to sign the Authorization.
- The potential for the PHI to be re-disclosed by the recipient and no longer protected by the Privacy Rule. This statement does not require an analysis of risk for re-disclosure but may be a general statement that the Privacy Rule may no longer protect health information.*

A research subject may revoke Authorization at any time. However, a covered entity may continue to use and disclose PHI that was obtained before the individual revoked Authorization to the extent that the entity has taken action in reliance on the Authorization. In cases where the research is conducted by the covered entity, this would permit the covered entity to continue using or disclosing the PHI as necessary to maintain the integrity of the research, as, for example, to account for a subject's withdrawal from the research study, to conduct investigations of scientific misconduct, or to report adverse events.

The next section of this document provides sample language and issues to consider in developing a research Authorization. The sample language addressing the required elements is listed first, followed by a set of optional elements that may be useful in specific research situations.

* If an Authorization permits disclosure of PHI to a person or organization that is not a covered entity (such as a sponsor or funding source of the research), the Privacy Rule does not continue to protect the PHI disclosed to the noncovered entity. However, other applicable Federal and State laws as well as agreements between the disclosing covered entity and the PHI recipient may establish continuing protections for the disclosed information.

SAMPLE AUTHORIZATION LANGUAGE FOR RESEARCH USES AND DISCLOSURES OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION BY A COVERED HEALTH CARE PROVIDER

Authorization to Use or Disclose (Release) Health Information that Identifies You for a Research Study

REQUIRED ELEMENTS:

If you sign this document, you give permission to [name or other identification of specific health care provider(s) or description of classes of persons, e.g., all doctors, all health care providers] at [name of covered entity or entities] to use or disclose (release) your health information that identifies you for the research study described here:

> [Provide a description of the research study, such as the title and purpose of the research.]

The health information that we may use or disclose (release) for this research includes [complete as appropriate]:

> [Provide a description of information to be used or disclosed for the research project. This may include, for example, all information in a medical record, results of physical examinations, medical history, lab tests, or certain health information indicating or relating to a particular condition.]

The health information listed above may be used by and/or disclosed (released) to:

> [Name or class of persons involved in the research; i.e., researchers and their staff *]

[Name of covered entity] is required by law to protect your health information. By signing this document, you authorize [name of covered entity] to use and/or disclose (release) your health information for this research. Those persons who receive your health information may not be required by Federal privacy laws (such as the Privacy Rule) to protect it and may share your information with others without your permission, if permitted by laws governing them.

---

* Where a covered entity conducts the research study, the Authorization must list ALL names or other identification, or ALL classes, of persons who will have access through the covered entity to the protected health information (PHI) for the research study (e.g., research collaborators, sponsors, and others who will have access to data that includes PHI). Examples may include, but are not limited to the following:

- Data coordinating centers that will receive and process PHI;
- Sponsors who want access to PHI or who will actually own the research data; and/or
- Institutional Review Boards or Data Safety and Monitoring Boards.

If the research study is conducted by an entity other than the covered entity, the authorization need only list the name or other identification of the outside researcher (or class of researchers) and any other entity to whom the covered entity is expected to make the disclosure.

Please note that [include the appropriate statement]:

- You do not have to sign this Authorization, but if you do not, you may not receive research-related treatment.
  (When the research involves treatment and is conducted by the covered entity or when the covered entity provides health care solely for the purpose of creating protected health information to disclose to a researcher).
- [Name of covered entity] may not condition (withhold or refuse) treating you on whether you sign this Authorization.
  (When the research does not involve research-related treatment by the covered entity or when the covered entity is not providing health care solely for the purpose of creating protected health information to disclose to a researcher)

Please note that [include the appropriate statement]:

- You may change your mind and revoke (take back) this Authorization at any time, except to the extent that [name of covered entity(ies)] has already acted based on this Authorization. To revoke this Authorization, you must write to: [name of the covered entity(ies) and contact information].
  (Where the research study is conducted by an entity other than the covered entity)
- You may change your mind and revoke (take back) this Authorization at any time. Even if you revoke this Authorization, [name or class of persons at the covered entity involved in the research] may still use or disclose health information they already have obtained about you as necessary to maintain the integrity or reliability of the current research. To revoke this Authorization, you must write to: [name of the covered entity(ies) and contact information].
  (Where the research study is conducted by the covered entity)

This Authorization does not have an expiration date [or as appropriate, insert expiration date or event, such as “end of the research study.”]

_____	_____
Signature of participant or participant’s personal representative	Date
_____	_____
Printed name of participant or participant’s personal representative	If applicable, a description of the personal representative’s authority to sign for the participant

SAMPLE AUTHORIZATION LANGUAGE FOR RESEARCH USES AND DISCLOSURES OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION BY A COVERED HEALTH CARE PROVIDER

AUTHORIZATION TO USE OR DISCLOSE (RELEASE) HEALTH INFORMATION THAT IDENTIFIES YOU FOR A RESEARCH STUDY

OPTIONAL ELEMENTS:

Examples of optional elements that may be relevant to the recipient of the protected health information:

- Your health information will be used or disclosed when required by law.
- Your health information may be shared with a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, and conducting public health surveillance, investigations, or interventions.
- No publication or public presentation about the research described above will reveal your identity without another authorization from you.
- If all information that does or can identify you is removed from your health information, the remaining information will no longer be subject to this authorization and may be used or disclosed for other purposes.
- **When the research for which the use or disclosure is made involves treatment and is conducted by a covered entity:** To maintain the integrity of this research study, you generally will not have access to your personal health information related to this research until the study is complete. At the conclusion of the research and at your request, you generally will have access to your health information that [name of the covered entity] maintains in a designated record set, which means a set of data that includes medical information or billing records used in whole or in part by your doctors or other health care providers at [name of the covered entity] to make decisions about individuals. Access to your health information in a designated record set is described in the Notice of Privacy Practices provided to you by [name of covered entity]. If it is necessary for your care, your health information will be provided to you or your physician.
- If you revoke this Authorization, you may no longer be allowed to participate in the research described in this Authorization.