

GUIDANCE ON THE HIPAA PRIVACY RULE FOR HUD OFFICE OF HEALTHY HOMES AND LEAD HAZARD CONTROL GRANTEEES

Key Points:

- The HIPAA Privacy Rule establishes a national standard of privacy protections for patients by limiting the ways that health plans, pharmacies, hospitals and other “covered entities” can use patients' personal medical information.
- Only “covered entities” have to comply with the HIPAA Privacy Rule. Covered entities include most health care providers (e.g., doctors and hospitals) and all health plans.
- A non-covered organization cannot become “covered” simply by getting data from a covered entity. Many organizations that use, collect, access, and share individually identifiable health information are not covered entities (i.e., they're not a health plan or covered hospital), and thus, do not have to comply with the HIPAA Privacy Rule.
- Complying with the HIPAA Privacy Rule means that covered entities must protect most individually identifiable health information that they hold and maintain from inappropriate use and disclosure. Covered entities must also implement standards for individuals' privacy rights to understand and control how their health information is used.
- The HIPAA Privacy Rule tells covered entities which uses and disclosures are allowed. For example, covered entities may use and share individually identifiable health information under certain conditions for specified public interest activities – such as when required by law, for public health activities, to avert a threat to health or safety, and for research.
- When in doubt about the applicability of the HIPAA Privacy Rule, remember to ask whether you are or work for a covered entity *before* you assess whether you handle individually identifiable health information. In addition, covered entities have a “Privacy Officer” to help answer questions about the HIPAA Privacy Rule.

What is the HIPAA Privacy Rule? The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996 to improve the portability and continuity of health care coverage. Part of the HIPAA legislation also required the government to issue a “HIPAA Privacy Rule” to make sure that individuals' health information is properly protected while it is being used and shared for health care and to protect the public's health and well being. The HIPAA Privacy Rule was published as “Standards for Privacy of Individually Identifiable Health Information” by the Department of Health and Human Services (HHS) for implementation by most affected entities in April 2003.

Do I have to follow the HIPAA Privacy Rule?

Possibly. The answer depends on whether you are (or you work for) a “covered entity.” A covered entity is a (1) health plan, (2) health care clearinghouse, or (3) health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard. A health care provider (e.g., doctor, nurse, community health center, or hospital) is a covered entity if it *electronically* transmits any health information concerning

billing and payment for services or insurance coverage, or other standard transaction. Covered entities can be institutions, organizations, or persons. For example, since many medical providers electronically transmit patient health information for billing or treatment purposes, many health care providers, such as medical centers and community health centers, are covered entities. For help in determining covered entity status, see the “decision tool” at www.hhs.gov/ocr/hipaa/.

If I’m a covered entity, what must I do to comply with the HIPAA Privacy Rule?

A covered entity must follow the HIPAA Privacy Rule (found at 45 CFR part 160 and Subparts A and E of part 164) to be in compliance. To follow the HIPAA Privacy Rule, a covered entity must implement the standards for protecting privacy when it uses and shares someone’s individually identifiable health information. In addition, the HIPAA Privacy Rule sets standards for individuals’ privacy rights to understand and control how their health information is used (i.e., patients can obtain a copy of their health information).

How does a covered entity know which information it needs to protect?

With limited exceptions, a covered entity must protect all individually identifiable health information it holds or maintains. This category of information affected by the HIPAA Privacy Rule is called “protected health information” or “PHI.” A covered entity must protect all forms of PHI – paper, electronic, and oral. The following algorithm is a good “rule of thumb” in determining if health information is protected by the HIPAA Privacy Rule.

Covered Entity + Health Information + Identifier = PHI

However, there are exceptions to this “rule of thumb.” For example, it is important to note that PHI may also include a covered entity’s list of patient names and addresses (without health information) and other demographic information.

If a covered entity removes the identifiers from health information (e.g., names and addresses) and makes “de-identified” health information, does the entity still have to protect that information?

The HIPAA Privacy Rule does not protect health information that is “de-identified.” Therefore, a covered entity may use or disclose such information without regard to the HIPAA Privacy Rule. One common way to de-identify PHI involves removing identifying information about the patient and his or her relatives, employers, or household members from the health information. Once these identifiers (see below) are removed, and the covered entity has no actual knowledge that the remaining information could be used to identify the individual; the health information is considered “de-identified” and is no longer PHI.

Names;
All geographic subdivisions smaller than a state;

All elements of dates (except year) directly related to an individual;

All ages over 89 and all elements of dates (including year) indicative of such age;
Telephone numbers;
Fax numbers;
E-mail addresses;
Medical record numbers;
Account numbers;
Certificate and license numbers;
Vehicle identifiers and serial numbers, including license plate numbers;

Medical device identifiers and serial numbers;
Web URLs;
IP addresses;
Biometric identifiers including fingerprints and voice prints;
Full-face photos and any comparable images;
Any other unique identifying number, characteristic, or code, unless otherwise permitted by the HIPAA Privacy Rule for re-identification.

I work for an Association that is not covered by the HIPAA Privacy Rule. If this Association receives individually identifiable health information from a covered community health center, does that mean this Association is now a covered entity?

No. The collection of individually identifiable health information is not a factor in determining whether a person, organization, or association is a covered entity. Covered entities are defined in HIPAA; they are (1) health plans, (2) health care clearinghouses, and (3) health care providers that transmit any health information in electronic form in connection with a transaction covered in the HIPAA Transactions Rule. An Association that meets none of these criteria, as defined at 45 CFR 160.103, is not a covered entity.

Can researchers be covered entities?

Yes, researchers may be covered entities. One way a researcher would be a covered health care provider is if he or she furnishes health care services to individuals, including the subjects of research, *and* transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule. See 45 CFR 160.102 and 160.103. For example, a researcher who conducts a study that involves the delivery of routine health care, such as blood lead level screening, *and* transmits health information in electronic form to a third party payer for payment, would be a covered health care provider under the HIPAA Privacy Rule.

Because a covered entity's workforce members must comply with the HIPAA Privacy Rule, a researcher may also have to follow the HIPAA Privacy Rule if he or she works for a covered entity, such as a covered medical center or community health center. The HIPAA Privacy Rule gives covered entities the option of requiring either all or some of its organization to comply with the HIPAA Privacy Rule. As a result, some covered entities may require all research activities performed by members of their staff or faculty to comply with the HIPAA Privacy Rule while other covered entities may not. For example, HUD OHHLHC grantees that work for organizations that provide patient care, such as community health centers, would come under HIPAA regulations if the community health center were a covered entity that requires those grantees to comply. Grantees are encouraged to contact their institution, IRB, counsel, or Privacy Officer to learn more about how the HIPAA Privacy Rule affects their institution.

What are some of the ways that a covered community health center can collect, use, and share identifiable lead hazard information from neighborhood families?

The HIPAA Privacy Rule provides several ways for covered entities, such as certain community health centers, to use and disclose PHI, such as identifiable lead hazard information. One way involves asking the individual to give their permission by signing an Authorization form.

Signed Authorization

An 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(s), stated in the authorization. For example, if a covered entity wants to conduct a research project using names and addresses of families having elevated blood lead levels; the covered entity would likely need to obtain each individual's authorization before using such identifiable information for research. In general, HUD OHHLHC grantees that work for covered entities usually obtain an individual's authorization for the research if the grantee interacts with the individual.

Research authorizations must be for a specific study and contain a series of core elements and required statements detailed at 45 CFR 164.508. It must include a description of the PHI to be used or disclosed; the person(s) authorized to make the requested use or disclosure; person(s) to whom the covered entity may disclose PHI; each purpose for the use or disclosure; the expiration date (or "none"); and the participant's signature. The authorization must also include information about the individual's right to revoke the authorization at any time and explain any exceptions to this right. For example, covered entities may continue to use or disclose PHI that was obtained before authorization was withdrawn, if necessary to maintain the integrity of the research study or to account for the subject's withdrawal.

Some institutions prefer to incorporate the authorization language into their informed consent document. If this is the policy of a grantee's institution, the IRB staff will be able to provide assistance in the creation of this joint form for your project. However, not all institutions or IRBs opt to incorporate the authorization into the informed consent document; your institution may require separate documents. If this is the case, again, you should consult your institution or IRB for advice on taking the necessary steps to prepare the authorization form. Although the HIPAA Privacy Rule does not require IRBs to review and approve authorization language, the Common Rule requires IRBs to review and approve informed consent language. As such, combined authorization-informed consent documents would undergo IRB review.

Required by Law

If a statute, regulation, court order, or other law requires covered entities to use and disclose PHI, the covered entity may make the use or disclosure without an individual's Authorization. For example, if a state law requires health care providers to report elevated blood lead levels to surveillance systems and public health authorities, a covered health care provider may disclose the necessary PHI to such authorities without obtaining the individual's authorization to do so.

Public Health Activities

The HIPAA Privacy Rule also recognizes that public health reports made by covered entities are an important means of identifying threats to the health and safety of the public at large, as well as individuals. Accordingly, the Rule permits covered entities to disclose PHI without authorization for specified public health purposes to public health authorities that are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury and conducting public health surveillance, investigations, or interventions. See 45 CFR 164.512(b)(1)(i).

A “public health authority” is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR 164.501. Examples of a public health authority include State and local public health departments, the Centers for Disease Control and Prevention (CDC), and anyone performing public health functions under a grant of authority from a public health agency. For those agencies and institutions that are covered entities under the HIPAA Privacy Rule, the Office of Healthy Homes and Lead Hazard Control, for the purpose of this program, is functioning as a public health authority as defined by 45 CFR 164.512. HUD, CDC, and the Environmental Protection Agency (EPA) are authorized by statute to conduct lead poisoning prevention activities, consistent with their missions and capabilities, to address the public health problem of lead poisoning and to coordinate these activities.

Avert a Serious Threat to Health or Safety

Covered entities may disclose PHI that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). For example, a covered community health center is permitted to share necessary PHI about a child’s elevated blood lead level with appropriate surveillance or public health authorities, without the authorization from the child’s parent(s), if doing so may prevent or lessen serious and imminent threat to the child’s safety.

Authorization Waiver for Research

While many HUD OHHLHC grantees that work for covered health care providers will obtain an individual’s authorization before using or sharing PHI for research, it may be impracticable under certain research circumstances (e.g., research involving only health records) for the covered entity to obtain the individual’s authorization. In such a case, the HIPAA Privacy Rule permits a covered entity to use or disclose the PHI for research if it has paperwork documenting an Institutional Review Board’s (IRB) decision to waive the authorization requirement. Thus, an IRB’s authority to act on waiver requests under the HIPAA Privacy Rule is in addition to the other authorities derived from the Common Rule and other applicable statutes and regulations. The HIPAA Privacy Rule does not alter IRB membership requirements, jurisdiction on matters concerning the protection of human subjects, or other procedural IRB matters.

As an alternative to obtaining authorization waivers from an IRB, a covered entity may obtain documentation that a properly constituted “Privacy Board” approved the waiver request for research. A Privacy Board must have (1) members with varying backgrounds and appropriate professional competencies as necessary to review the effect of the research protocol on individuals' privacy rights and related interests, (2) 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, and (3) members without conflicts of interest regarding the projects they review.

Where both an IRB and Privacy Board coexist, the HIPAA Privacy Rule does *not* require approval of a waiver of Authorization by both bodies because a covered entity may rely on waiver documentation by any IRB or Privacy Board, without regard to the location of the approver. As such, a covered entity may rely on documentation from any independent, local, or central Privacy Board or IRBs.

Health information with only dates and certain address information

For certain activities (e.g., for research and public health), a covered entity may use and share PHI without needing to get authorization of a waiver of authorization if direct identifiers have been removed from the health information. This type of PHI is called a “limited data set.” For example, a covered entity can retain, use, and share all dates and ages and most geographic information (such as city, state, ZIP code, county, and precinct) in a limited data set as long as the covered entity has established with the data recipient a data use agreement -- an assurance that the limited data set recipient will use or disclose the PHI only for specified purposes. The table below provides examples to distinguish between de-identified data, a limited data set, and a data set containing direct identifiers.

Fully Identifiable Data	Limited Data Set	De-identified Data
<p>Jane Doe 1234 Main Street Big Town, AZ 12345 (123) 456-7890</p> <p>Blood Pressure: 120/80 Heart Rate: 60 beats/min</p> <p>Date of Tests: January 1, 2001</p> <p><i>Can use with authorization or waiver of authorization (for example). Refer to the HIPAA Privacy Rule for more permitted uses and disclosures of such PHI.</i></p>	<p>Big Town, AZ 12345</p> <p>Blood Pressure: 120/80 Heart Rate: 60 beats/min</p> <p>Date of Tests: January 1, 2001</p> <p><i>Can use with a data use agreement (authorization and waiver of authorization not needed).</i></p>	<p>Blood Pressure: 120/80 Heart Rate: 60 beats/min</p> <p><i>No HIPAA Privacy Rule permissions needed for “de-identified” data.</i></p>

How do I know if my project involving healthy homes is “research?”

Research is defined in the HIPAA Privacy Rule as “a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.” (45 CFR 164.501). This is similar to the Protection of Human Subjects definition of research, commonly known as the “Common Rule” that was adopted by HUD (24 CFR 60.101). The Common Rule defines research as “a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program that is considered research for other purposes. For example, some demonstration and service programs may include research activities.” (45 CFR 46.102). The HIPAA Privacy Rule does not replace or modify the Common Rule, so HUD grantees that are also covered entities may have to comply with both sets of regulations.

My community health center funds an Industrial Hygiene Firm to remediate mold hazards and perform Integrated Pest Management as part of our healthy homes demonstration research project. Data documenting the results of these activities is incorporated into our database and contributes to our research findings. We provide the Hygiene Firm with the patient’s names and addresses. Does this research collaboration make the Hygiene Firm our business associate because they’re collecting information “for” us?

No. Research itself is not a function that would require a covered entity (e.g., the covered community health center) to enter into a business associate relationship with a collaborator who, for example, conducts research for or on behalf of a covered entity. Therefore, even though PHI exchanges hands between a covered entity and a research collaborator, a business associate agreement is unnecessary. However, other HIPAA Privacy Rule requirements would apply to the covered entity’s disclosure of such information. For example, the covered entity may need to obtain authorization from the individuals.

Additional Information about the HIPAA Privacy Rule can be found on the following web sites:

Office for Civil Rights (OCR), 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/privacyrule/>

Food and Drug Administration (FDA)

<http://www.fda.gov/>

National Institutes of Health (NIH)

<http://privacyruleandresearch.nih.gov>

Office for Human Research Protections (OHRP), HHS

<http://ohrp.osophs.dhhs.gov/>

Centers for Medicare and Medicaid Services (CMS), HHS

<http://www.cms.hhs.gov/hipaa/>

Glossary of HIPAA Terms:

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 HIPAA Privacy Rule, a Covered Entity may not use or disclose PHI for research purposes without a valid Authorization.

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.

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.

Disclosure - The release, transfer, access to, or divulging of information in any other manner outside the Covered Entity holding the information.

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 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.

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.

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.

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.

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.

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.