SPECTRUM HEALTH
Human Research Protection Program
Office of the Institutional Review Board
100 Michigan NE, MC 038
Grand Rapids, MI 49503
616.486.2031
irb@spectrumhealth.org
www.spectrumhealth.org/HRPP

HIPAA & Research: Frequently Asked Questions

A Spectrum Health IRB Guidance Document

Purpose

This document provides guidance on many common questions the IRB receives related to HIPAA. Contact the IRB office at (616) 486-2031 or irbassist@spectrumhealth.org if you have additional questions or need assistance applying HIPAA to your research project.

FAQs

1. *What is the definition of …?*
   - **Individually Identifiable Health Information:** A subset of health information that identifies the individual or can reasonably be used to identify the individual. [45 CFR 160.103]

   - **Protected Health Information (PHI):** Individually identifiable health information that is transmitted or maintained in any form by a covered entity. [45 CFR 160.103]

- **Limited Data Set**: A "limited data set" is a limited set of identifiable patient information as defined in the HIPAA Privacy Rule. A "limited data set" of information may be disclosed to an outside party without a patient's authorization if certain conditions are met. First, the purpose of the disclosure may only be for research, public health or health care operations. Second, the person or organization receiving the information must sign a data use agreement. Specifically, as it relates to the individual or his or her relatives, employers or household members, **all the following identifiers must be removed in order for health information to be a "limited data set":**
    - names;
    - street addresses (other than town, city, state and zip code);
    - telephone numbers;
    - fax numbers;
    - e-mail addresses;
    - Social Security numbers;
    - medical records numbers;
    - health plan beneficiary numbers;
    - account numbers;
    - certificate license numbers;
    - vehicle identifiers and serial numbers, including license plates;
    - device identifiers and serial numbers;
    - URLs;
    - IP address numbers;
    - biometric identifiers (including finger and voice prints); and
    - full face photos (or comparable images)

  The health information that may remain in a limited data set includes**:**
    - dates, such as date of admission, discharge, service, DOB, DOD;
    - city, state, five digit or more zip code; and
    - ages in years, months, days or hours.

  It is important to note that this information is still protected health information or "PHI" under HIPAA. It is not de-identified information and is still subject to the requirements of the Privacy Rule. [45 CFR 164.514(e)]

- **De-identified Data:** Under the HIPAA Privacy Rule, data are de-identified if either (1) an expert determines that the risk that certain information could be used to identify an individual is "very small" and documents and justifies the determination, or (2) the data do not include any of the eighteen identifiers (of the individual or his/her relatives, household members, or employers) which could be used alone or in combination with other information to identify the individual. Note that even if these identifiers are removed, the Privacy Rule states that information will be considered identifiable if the covered entity knows that the identity of the person may still be determined. [45 CFR 164.514(a)(b)]

2. *Who has to follow HIPAA regulations? Who is not required to follow these laws?*
   The entities that must follow the HIPAA regulations are called ***covered entities***. [45 CFR 160.102]

Covered entities include:

- Health Plans, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.
- Most Health Care Providers—those that conduct certain business electronically, such as electronically billing your health insurance. Thisincludes most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.
- Health Care Clearinghouses—entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

  [45 CFR 160.103]

Under the HITECH Act (enacted as part of the American Recovery and Reinvestment Act of 2009), ***business associates*** (discussed in Question 11) must also comply with HIPAA regulations.

While many organizations that have health information about individuals do not have to follow these laws, certain other protective laws are applicable to them. Examples of organizations that may not have to follow the HIPAA Privacy and Security Rules include:

- life insurers
- employers
- workers compensation carriers
- many schools and school districts
- many state agencies like child protective service agencies
- many law enforcement agencies
- many municipal offices

3. *When does HIPAA apply to my research?*
   HIPAA applies to your research anytime you are accessing, using, recording, and/or receiving identifiable patient information from a covered entity. The key word here is "identifiable" patient information. If you are receiving a de-identified data set (stripped of all 18 identifiers) then you do not need a waiver or individual authorization from each patient to use the data for research purposes. Also, HIPAA does not apply to your research if it does not involve any health information from a covered entity (e.g. a survey on TV viewing habits at home and the correlation between school tardiness).

   The majority of research conducted at Spectrum Health (a covered entity) involves the use of identifiable patient information and thus requires either a valid data use agreement, HIPAA waiver, or individual patient authorization to be able to conduct the research. [45 CFR 164 Subpart E]

4. *What do I need to include in my HIPAA authorization?*
   HIPAA Authorizations must be written in plain language and must include 6 core elements and three required statements. Refer to pages 7-9 of the Informed Consent Form template (www.spectrumhealth.org/irbforms) and 45 CFR Part 164.508(c)(1)(2).

5. *When do I need to list the FDA in the HIPAA authorization?*
   Anytime you are conducting a research study or registry investigating the safety and efficacy/effectiveness of a drug or medical device (experimental or FDA approved/cleared) you should list the FDA under who may use or see/share the subjects' protected health information.

6. *Do I have to obtain HIPAA authorization in writing? Is it okay if the individual gives me verbal authorization?*
   Obtaining verbal HIPAA authorization is permitted as long as the Privacy Board has waived the requirement to obtain a signed authorization. This alteration is allowable only when certain conditions are met; for example, the research must involve no more than minimal risk. You may still be required to provide an information sheet containing all the required elements of HIPAA authorization to the individual. If verbal authorization will be obtained over the phone, you must read the authorization to the individual. When obtaining verbal authorization, you are still expected to record in your study documents/phone script who provided verbal authorization (individual's or parent/legally authorized representative's name), when (the date), and who obtained it (researcher/research assistant's name). A waiver of documentation is not equivalent to a complete waiver of HIPAA authorization. [45 CFR 164.512(i)(2)(ii)]

7. *When can I access medical records for recruiting patients and protocol development without a HIPAA waiver or authorization?*
   The HIPAA regulations allow medical records to be accessed for reviews preparatory to research without a waiver or authorization, provided certain criteria are met. These preparatory activities include protocol development, identification of prospective research participants, and study recruitment. However, this provision does not permit the researcher to remove information from the covered entity. A researcher who is an employee or a member of the covered entity's workforce can use protected health information to contact prospective research subjects. However, a researcher who is not a part of the covered entity may not use the preparatory research provision to contact prospective research subjects. [45 CFR 164.512(i)(1)(ii) & www.dhhs.gov/hipaafaq/permitted/research/317.html]

8. *How can my research qualify for a waiver of HIPAA authorization?*
   In general*, a researcher may qualify for a waiver of individual patient authorization if the following conditions below are met.
   1) The researcher takes steps to minimize a possible breach of confidentiality (i.e. the spreadsheet/database itself and computers are password protected and/or encrypted; the correlation tool or identifiable information in the spreadsheet/database will be destroyed when the research is complete or shortly after accepted for publication; research staff have had HIPAA training).
   2) The researcher successfully argues the research could not practicably be conducted without the waiver or alteration. Keep in mind here, stating in your application that requiring individual authorization would take too much time and incur additional cost is not adequate for granting a waiver. More appropriate arguments to consider are:
      a) scientific validity could be compromised by requiring authorization because only including those medical records for which authorization could be obtained would prohibit conclusions to be drawn or create a bias that may skew the data; or
      b) locating the potential patients would be very difficult due to a significant percentage of the population being studied would be lost to follow-up, relocated or deceased, and including only those able to be contacted may result in the study may not be meaningful or lose statistical power; or
      c) ethically it may be best to not contact the individual for authorization because there is increased risk in creating a list of contact information associated with the research study

question; or there is a risk of inflicting additional psychological, social, or other harm when contacting the individual about participation or their families in the case of minors

*There are exceptions that do not qualify for granting a waiver, such as recording positive HIV status as part of the research.

[45 CFR Part 164 Subpart E(i) Standard: Uses and disclosures for research purposes; OHRP SACRHP Letter to HHS Secretary January 31, 2008, Recommendations related to waiver of consent]

9. *Does the withdrawal of authorization have to be in writing?*
   Yes, valid withdrawals must be in writing. This can be an email, a mailed letter, or a fax. If a participant withdraws from a research study, this does not automatically cancel the HIPAA authorization. [45CFR164.508(c)(2)(i)]

10. *Can I look at the medical records of decedents for research purposes?*
    Yes, once you have submitted FORM: Investigator's Attestation: Research Using Decedent Protected Health Information (HRP-203). This document can be found on our website www.spectrumhealth.org/irbforms. Once completed, forward it to irb@spectrumhealth.org.
    [45 CFR 164.512(i)(1)(iii)]

11. *What is a Business Associate Agreement?*
    A Business Associate Agreement (BAA) is a legal contract created between an outside person or organization providing services for a covered entity (e.g. Spectrum Health). A BAA lists the terms and conditions the business associate must follow when using and releasing PHI. Business associates may provide health care services or legal, consulting, actuarial, administrative, accreditation and financial services for the covered entity.

    In most cases, disclosing PHI to an outside researcher for research purposes does not require a BAA. This is because the researcher is not conducting a service for the covered entity and thus the researcher is not considered a "business associate." Instead, a Data Use Agreement (DUA), study/clinical trial agreement (CTA), waiver, and/or individual authorization may be required depending on the type of research.

    Also, a BAA is typically not required with collaborating research institutions, coordinating centers, study sponsors, statistical centers, and data monitoring boards. Instead, the study/clinical trial contract between Spectrum Health and the collaborating institution or study sponsor takes into account HIPAA-related privacy and security issues.
    [OCR HIPAA Privacy *December 3, 2002 Revised April 3, 2003*]
    [BUSINESS ASSOCIATES *45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)*]

12. *Do I need a HIPAA waiver if my project is quality?*
    No. This is covered under the general consent to treatment which is signed by patients at time of service. It allows the use and disclosure of PHI for treatment, payment, and health care operations. Health care operations include various activities that improve the quality of care received (QI and QA projects). [45 CFR 164.506]