Sentara Health Research Center

Research and the HIPAA Privacy Rule

In response to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the U.S. Department of Health and Human Services (HHS) issued the regulations "Standards for Privacy of Individually Identifiable Health Information." These regulations, known as "The Privacy Rule," went into effect on April 14, 2003.

The HIPAA Privacy Rule regulates the way certain healthcare groups, organizations, or businesses, called "covered entities," manage individually identifiable health information called "protected health information" (PHI). The Privacy Rule pertains to both the use of PHI and disclosure of PHI. Breaches of the Privacy Rule are subject to investigation by the HHS Office of Civil Rights. Any potential or suspected inappropriate access, use or disclosure of Sentara's PHI must be reported to the Sentara Privacy Officer to ensure the HIPAA Breach Notification requirements are met.

A covered entity includes any healthcare entity that transmits health information electronically in connection with certain financial and administrative transactions, including health plans, healthcare clearing houses, and health care providers that electronically transmit health information. Employees or workforce members of a covered entity who are involved in research are expected to comply with that entity's HIPAA Privacy policies and procedures. The Privacy Rule applies to covered entities and not to research or researchers per se. However, an individual researcher may be considered a covered entity if he or she is a firm that independently engages in any of the covered electronic transactions.

PHI is a subset of individually identifiable health information that is created, transmitted, or maintained in electronic or any other form or medium by a covered entity. Individually identifiable health information includes both direct identifiers such as names and MRNs, and indirect identifiers such as zip codes and admission dates.

Deidentified data is not PHI and is not protected under the Privacy Rule. PHI can be de-identified by removal of all 18 identifying elements (the "safe harbor" method) or by using statistical verification of deidentification by a qualified statistician with appropriate knowledge and experience (45 CFR 164.502 (d) and 164.514(a)-(c) of the Rule). Research using pre-existing databases of deidentified data is not considered human subjects research and is not subject to IRB approval if the individuals cannot be re-identified either directly or through indirect identifiers (like zip codes and service dates) linked to individual subjects.

The Privacy Rule describes the conditions under which a covered entity can either use or disclose PHI. "Use" is the sharing, employment, application, utilization, examination, or analysis of PHI. "Disclosure" is the release, transfer, provision of access to, or divulging in any manner of PHI.
The Use or Disclosure of PHI for non-treatment related activities must adhere to the "Minimum Necessary" requirement whereby a covered entity must apply policies, procedures, or criteria to limit certain uses or disclosures of PHI to "the information reasonably necessary to accomplish the purpose."

PHI may be used and disclosed for research under the following conditions:

- With an individual's permission in the form of a written Authorization. An Authorization is different from informed consent in that it focuses on privacy risks and states how, why, and to whom the PHI will be used and/or disclosed for research. It is a signed permission with an expiration data that pertains to a specific research study. An Authorization may be combined with informed consent in a single document.
- For activities preparatory to research. For this use, a covered entity must obtain from a researcher oral or written representation that, 1. The use is solely to prepare a research protocol or for other purposes preparatory to research, 2. The PHI will used on site and will not be removed from the covered entity in the course of review, and 3. The PHI is necessary for research, such as to aid study recruitment or determining whether a sufficient number or type of records exists to conduct the research. This use may help the researcher prepare a research protocol, develop a research hypothesis, or identify potential study participants. While the Privacy Rule allows either an oral or written representation from a researcher, Sentara requires all such representations in writing.
- For research on decedents' information.
- When Authorization has been waived by an IRB or a Privacy Board. A waiver must satisfy the following criteria:
    1. Use of the PHI involves no more than minimal risk to the privacy of individuals based on:
        B. An adequate plan to protect PHI identifiers from improper use or disclosure.
        C. An adequate plan to destroy PHI at earliest opportunity consistent with the conduct of research
        D. Adequate written assurances that PHI will not be reused or disclosed to any other person or entity or used for other research purposes.
    2. The research could not be practicably conducted without the waiver.
    3. The research could not be practicably conducted without access to and use of the PHI.
- If PHI is in the form of a Limited Data Set, which refers to PHI that excludes 16 categories of direct identifiers.
    - A Limited Data Set can include homelocation including city, state, zip code, precincts, and geocodes but may not include street name, number or PO Box number. It can also include all elements of dates, including admission, discharge, and service dates, dates of birth, and if applicable, date of death, and age.
    - Disclosure of a limited data set requires a Data Use Agreement (DUA), which describes the purpose, the identity of those permitted to use the limited data set, who will not use it, appropriate safeguards, and agreement to not add back identifiers.

- If the PHI is based on a permission that predates the applicable compliance date of the Privacy Rule (April 14, 2003).
- Other limited uses of PHI such as cancer registries if disclosure is required by law.
- Disclosure to a public health authority that is authorized by law to receive information for the purpose of preventing or controlling disease, injury, or disability.
- Disclosure to the FDA for purposes related to quality, safety, or effectiveness of an FDA-regulated product, to health oversight agencies for oversight of government-regulated programs.

If research involves only the analysis of pre-existing data that has already been fully de-identified for general purposes according to the HIPAA standard, an IRB application is not required because the research does not involve either PHI or an identifiable human subject. However, if a researcher wishes to extract de-identified data from the medical record or other identifiable sources for use in research, or to create a de-identified database for future general research, the researcher must submit an IRB protocol asking for a waiver of HIPAA Privacy Authorization satisfying the criteria listed above. If data has been de-identified under an IRB-approved protocol for a specific purpose, the de-deidentified data cannot be reused for another purpose without additional IRB approval. Use or disclosure of PHI to create a research database or repository and use or disclosure of PHI from a data base or repository are each considered separate research activities and require separate IRB protocols and waivers of Authorization under the Privacy Rule.

HIPAA permits the use of unique identifying codes or other means of record identification in a de-identified data set, provided that the researcher has no access to the linking code and no means of reidentifying the data. If the link is known, the identifier becomes PHI. If the link is destroyed, the data becomes de-identified for all purposes.

A covered entity can disclose PHI to a Business Associate, which is a person or entity conducting certain functions on behalf of a coveredentity, such as outside lawyers, consultants or contractors. This is covered under a Business Associate Agreement (BAA) and a Contract specifying the terms of the services the Business Associate will perform on behalf of the covered entity. A researcher or research sponsor is not required to become a business associate of a covered entity for research purposes. Outside parties that are involved in a research study and are listed the IRB protocol are not considered business associates, as they are necessarily involved in the common enterprise of a research project.

A researcher may contact potential study participants without Authorization from the individual if the researcher is a workforce member of a covered entity and the contact is part of a covered entity's normal operations for the purpose of seeking Authorization, or the covered entity obtains documentation that an IRB has waived Authorization to disclose PHI to a researcher for recruitment purposes. The Privacy Rule permits a covered entity to provide researchers access to PHI for identifying potential study patients provided that the covered entity receives oral or written representations from the researcher that the

researcher will not remove any PHI from the covered entity during the course of the review. While the Privacy Rule allows either an oral or written representation from a researcher, Sentara requires all such representations in writing.

The HIPAA Security Rule is a regulation separate from the Privacy Rule. The Privacy Rule applies to all identifiable health information created and maintained by a covered entity regardless of the medium. The Security Rule establishes standards for how covered entities store, transmit and safeguard "ePHI." Remote access to PHI and transmission of PHI outside of Sentara is also governed by the Sentara External Data Sharing Policy and is governed by the Operational Data Governance Council (ODGC), which meets quarterly. According to this policy, "data requested by HADSI/EVMS for research purposes are covered under specific sharing agreements with EVMS and will be reviewed for conformance by the Quality Research Institute within Enterprise Analytics, or by a larger Sentara Research Organization, should such an organization be established." Any potential security breaches must be reported to the Sentara Chief Information Security Officer and/or the Sentara Privacy Officer.

Some outcomes researchers may design a study that engages patients to collect Patient Reported Outcomes (PRO) and other information (such as biomedical data from wearable detectors) directly from an individual. Contacting and engaging patients for research conducted in this manner is human subjects research and requires IRB approval. The self-reported data is confidential information and must be treated carefully, but data collected directly from patients through self-reported research surveys is not considered PHI.The HITECH and 21st Century Cures Act have expanded HIPAA's regulations to allow patients greater ownership and access to their electronic data. Protected health information from EHRs and other sources can be accessed directly by patients through patient-facing application programming interfaces (APIs) or patient portals. Electronic platforms have been developed for researchers that allow patients to directly participate in research by accessing their PHI and porting that information to a confidential research database. Because the data is released directly to the patient under the patient's authorization, such data is no longer PHI according to the Privacy Rule.

Case reports are unsystematic clinical observations used for educational purposes and do not meet the Common Rule's definition of research. Thus, case reports do not require IRB approval. Case reports require written Authorization from the patient if they include PHI. Case reports do not require Authorization if identifiersa are removed, but caution should be used if the case is a unique or rare case where the patient could still be identifiable. In such cases, a signed Authorization may still be required.

Identifiers that must be removed by a covered entity to de-indentify data:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographic 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:
    - The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people
    - The initial three digits of a ZIP Code for all such geographic units containing 20,000 fewer people are changed to 000
- 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
- Telephone numbers
- Facsimile number
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code unless otherwise permitted by the Privacy Rule for re-identification

Identifiers that must be removed by a covered entity to create a Limited Data Set:

- Names
- Postal address information, other than town or city, state, and ZIP Code
- Telephone numbers
- Facsimile number
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographic images and any comparable images