What is Covered by HIPAA at VCU?

The Health Insurance Portability and Accountability Act of 1996, or "HIPAA" as most know it, is covered in the context of what it is and how it plays out in our unique environment in the information below.

In summary, HIPAA provides certain security and privacy protections for patient health information. In the VCU and VCU Health System environments, HIPAA may be applicable in a variety of circumstances depending on the context. For example, what parties are involved, their relationship and what activities wish to be, or are already being, conducted. Privacy, and how sensitive and personal information in our healthcare and the research environments is addressed.

As you know, the information used in research and patient care is highly regulated. The information may be patient **protected health information (PHI)**, governed by the Health Information Portability and Accountability Act (HIPAA), or it may be deemed **research health information (RHI)** after appropriate IRB and Privacy Board approvals are properly obtained. Whatever the legal or regulatory requirements, understanding the authorized uses and disclosures of this information can get complex in our VCU and VCU Health worlds; therefore, it is critical to ask questions to ensure your understanding before taking action with any information.

HIPAA BACKGROUND – The BASICS and the WHY

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) covers both **security** of patient information and **privacy** of patients' individual identifiable health information. Health and Human Services describes HIPPA as providing federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. HIPAA uses the term: individually identifiable health information, often referred to as PHI which means PROTECTED HEALTH INFORMATION.

HHS published a final rule to improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

- HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

VCU HAS HYBRID ENTITY STATUS.

Because VCU has both health care components and non-health care components, it is considered **a hybrid entity** under HIPAA regulation. That means VCU must be clear about its **covered components** as a **hybrid entity.** VCU's hybrid status and its close working relationship with the VCU Health System Authority has resulted in an agreed to structure called the **Affiliated Covered Entity (ACE)** so that common policies and practices may be used for HIPAA compliance and so that the flow of all patient information may continue as seamlessly between the two separate legal entities as the HIPAA regulations permit.

VCU and VCUHS are jointly covered by HIPAA regulations under what is termed the **VCU Affiliated Covered Entity (VCU ACE)**. All of the units included in the VCU ACE may have access to Protected Health Information through the conduct of standard business operations. The VCU ACE includes the following units:

- VCU Health System & all satellite clinics
- School of Medicine
- School of Pharmacy
- School of Nursing
- School of Dentistry
- College of Health Professions
- VCU Employee Health
- VCU Telecommunications
- VCU Audit & Compliance Services
- VCU Police Services
- VCU Office of University Counsel
- VCU Office of the VP for Research & Innovation

WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

HIPAA's Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."[12]

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

WHAT IS RESEARCH HEALTH INFORMATION (RHI)?

In contrast, some research studies may use health-related information that is personally identifiable because it includes personal identifiers such as name or address, but it is not considered to be PHI because the data are not associated with or derived from a healthcare service event (treatment, payment, operations, medical records) and the data are not entered into the medical records. HIPAA

does not apply to “research health information” (RHI) that is kept only in the researcher’s records; however, other human subjects protection regulations still apply.

Examples of research using only RHI and thus not subject to HIPAA include: use of aggregated (non-individual) data; diagnostic tests from which results are not entered into the medical record and are not disclosed to the subject; and testing conducted without any PHI identifiers. Some genetic basic research can fall into this category, such as the search for potential genetic markers, promoter control elements, and other exploratory genetic research. In contrast, genetic testing for a known disease, as part of diagnosis, treatment, and health care, would be considered a use of PHI and therefore subject to HIPAA regulations.

Also note, health information by itself without the 18 identifiers is not considered to be PHI. For example, a data set of vital signs by themselves does not constitute protected health information. However, if the vital signs data set includes medical record numbers, then the entire data set is considered PHI and must be protected since it contains an identifier.

De-Identified Health Information.

There are no restrictions on the use or disclosure of de-identified health information.[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual’s relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed to achieve the “safe harbor” method of de-identification:

1. Names;
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census:
    i. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    ii. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is 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. Phone numbers;
5. Fax 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 finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

In addition to the removal of the 18-listed identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information. 45 C.F.R. § 164.514(b).

There are also additional standards and criteria to protect individuals from re-identification. Any code used to replace the identifiers in data sets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. For example, a subject's initials cannot be used to code their data because the initials are derived from their name.

Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study. In other words, the information would still be considered identifiable if there was a way to identify the individual even though all of the 18 identifiers were removed.

HOW CAN THE HEALTH SYSTEM'S PATIENT INFORMATION BE USED FOR RESEARCH PURPOSES?

Researchers who want to access, collect, or otherwise use the Health System's PHI for research will need to follow a specific pathway for use as allowed by the HIPAA Privacy Rule, regardless of the role played at VCU. Even health care providers within the ACE cannot access or use ACE's patient's PHI about their own patients for research unless following one of the pathways outlined below.

In the course of conducting research, researchers may obtain, create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose protected health information for research with individual authorization, or without individual authorization under limited circumstances set forth in the Privacy Rule. Research Use/Disclosure Without Authorization. To use or disclose protected health information without authorization by the research participant, a covered entity must obtain one of the following:

A. Research Use/Disclosure with Individual Authorization.

The Privacy Rule also permits covered entities to use or disclose protected health information for research purposes when a research participant authorizes the use or disclosure of information about him or herself. Today, for example, a research participant's authorization will typically be

sought for most clinical trials and some records research. In this case, documentation of IRB or Privacy Board approval of a waiver of authorization is not required for the use or disclosure of protected health information. To use or disclose protected health information with authorization by the research participant, the covered entity must obtain an authorization that satisfies the requirements of 45 CFR 164.508. The Privacy Rule has a general set of authorization requirements that apply to all uses and disclosures, including those for research purposes. However, several special provisions apply to research authorizations:

- Unlike other authorizations, an authorization for a research purpose may state that the authorization does not expire, that there is no expiration date or event, or that the authorization continues until the "end of the research study".
- An authorization for the use or disclosure of protected health information for a research study may be combined with a consent to participate in the research, or with any other legal permission related to the research study.
- An authorization for the use or disclosure of protected health information for a research study may be combined with an authorization for a different research activity, provided that, if research-related treatment is conditioned on the provision of one of the authorizations, such as in the context of a clinical trial, then the compound authorization must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the unconditioned research activity.
- An authorization may be obtained from an individual for uses and disclosures of protected health information for future research purposes, so long as the authorization adequately describes the future research such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for the future research purposes.
- New Guidance on HIPAA and individual authorization of uses and disclosures of protected health information for research. - PDF This guidance explains certain requirements for an authorization to use or disclose PHI **for future research**. The guidance also clarifies aspects of the individual's right to revoke an authorization for research uses and disclosures of PHI.

B. Waiver or Alteration of Authorization.

Documentation that an alteration or waiver of research participants' authorization for use/disclosure of information about them for research purposes has been approved by an IRB or a Privacy Board. See 45 CFR 164.512(i)(1)(i). This provision of the Privacy Rule might be used, for example, to conduct records research, when researchers are unable to use de-identified information, and the research could not practicably be conducted if research participants' authorization were required.

A covered entity may use or disclose protected health information for research purposes pursuant to a waiver of authorization by an IRB or Privacy Board, provided it has obtained documentation of all of the following:

- Identification of the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;

- A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the three criteria in the Rule;
- A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or Privacy Board;
- A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and
- The signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.

The following three criteria must be satisfied for an IRB or Privacy Board to approve a waiver of authorization under the Privacy Rule:

1. The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
    - an adequate plan to protect the identifiers from improper use and disclosure;
    - an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
    - adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;
2. The research could not practicably be conducted without the waiver or alteration; and
3. The research could not practicably be conducted without access to and use of the PHI.

C. Preparatory to Research Documentation.

Representations from the researcher, either in writing or orally, that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any protected health information from the covered entity, and representation that protected health information for which access is sought is necessary for the research purpose. See 45 CFR 164.512(i)(1)(ii).

- This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study. The Privacy Rule does not prohibit a covered entity's granting remote access to PHI to a researcher for activities that qualify as reviews preparatory to research, provided reasonable and appropriate safeguards are in place, as described in OCR's guidance, Remote Access to PHI for Activities Preparatory to Research.

D. Research on PHI of Decedents Documentation.

Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought. See 45 CFR 164.512(i)(1)(iii).

E. Limited Data Sets with a Data Use Agreement.

A data use agreement entered into by both the covered entity and the researcher, pursuant to which the covered entity may disclose a limited data set to the researcher. See 45 CFR 164.514(e). A limited data set excludes specified direct identifiers of the individual or of relatives, employers, or household members of the individual. The data use agreement must:

- Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the Rule if done by the covered entity;
- Limit who can use or receive the data; and
- Require the recipient to agree to the following:
  - Not to use or disclose the information other than as permitted by the data use agreement or as otherwise required by law;
  - Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the data use agreement;
  - Report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which the recipient becomes aware;
  - Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; and
  - Not to identify the information or contact the individual.

ACCOUNTING FOR RESEARCH DISCLOSURES

In general, the Privacy Rule gives individuals the right to receive an accounting of certain disclosures of protected health information made by a covered entity. See 45 CFR 164.528. This accounting must include disclosures of protected health information that occurred during the six years prior to the individual's request for an accounting, or since the applicable compliance date (whichever is sooner), and must include specified information regarding each disclosure. A more general accounting is permitted for subsequent multiple disclosures to the same person or entity for a single purpose. See 45 CFR 164.528(b)(3).

Among the types of disclosures that are exempt from this accounting requirement are:

- Research disclosures made pursuant to an individual's authorization;
- Disclosures of the limited data set to researchers with a data use agreement under 45 CFR 164.514(e).

In addition, for disclosures of protected health information for research purposes without the individual's authorization pursuant to 45 CFR164.512(i), and that involve at least 50 records, the Privacy Rule allows for a simplified accounting of such disclosures by covered entities. Under this simplified accounting provision, covered entities may provide individuals with a list of all protocols for which the patient's protected health information may have been disclosed under 45 CFR 164.512(i), as well as the researcher's name and contact information. Other requirements related to this simplified accounting provision are found in 45 CFR 164.528(b)(4).

If you'd like to know more, consider Signing Up for the OCR Privacy & Security Listservs

HHS's OCR has established two listservs to inform the public about health information privacy and security FAQs, guidance, and technical assistance materials. You are encouraged to sign up and stay informed!

The IRB/Privacy Board Office within the VP's Office of Research and Innovation is here to support you in any role you hold. Never hesitate to ask questions or provide us feedback so we can continuously improve these operations and VCU's activities.

TABLE COMPARING PATHWAYS FOR ACCESSING AND USING PHI

De-Identified Data	**Review Preparatory to Research** (VCU PHI only)	**Limited Data Set and Data Use Agreement**	**Research with Decedent PHI** (VCU PHI only)	**Signed HIPAA Authorization**	**Partial Waiver of Authorization**	**Waiver of Authorization**
Affected Research Activities	Affected Research Activities	Affected Research Activities	Affected Research Activities	Affected Research Activities	Affected Research Activities	Affected Research Activities
All research – related activities involving PHI where data is recorded without any of the 18 identifiers	Accessing PHI held by the VCU ACE to **determine feasibility** (# of possible research participants available) Only needed when determining feasibility requires researcher to review identifiable health information	Any PHI data where some specific indirect identifiers are sufficient – see below • The VCU data use agreement only applies to PHI collected from within the VCU ACE • Other covered entities (e.g., private physicians) may require their own data use agreement	Any PHI data from within the VCU ACE pertaining to decedents	All research activities involving PHI where none of the other pathways apply	1. Accessing PHI to identify potential participants for **recruitment** with intent to obtain signed authorization upon enrollment 2. Request to waive one or more required elements of Authorization, such as signature when documentation of Authorization is not practicable.	Research activities involving PHI where preceding pathways are not possible **AND** it is not practicable to obtain signed authorization Generally appropriate under the same circumstances as waiver of consent

De-Identified Data	**Review Preparatory to Research** (VCU PHI only)	**Limited Data Set and Data Use Agreement**	**Research with Decedent PHI** (VCU PHI only)	**Signed HIPAA Authorization**	**Partial Waiver of Authorization**	**Waiver of Authorization**
How to Use PHI	How to Use PHI	How to Use PHI	How to Use PHI	How to Use PHI	How to Use PHI	How to Use PHI
Not subject to HIPAA if 1 of 2 options is followed. Option 1: May not record any of the 18 HIPAA identifiers. A unique code not derived from any of the 18 identifiers may be associated with the data. The researcher may not have access to the key to the code. Option 2: Use statistical methods to render the information not individually identifiable. Must submit a written certification from a qualified statistician to HRPP that the risk of reidentification is "very small".	Submit Review Preparatory to Research Form to HRPP in REDCap. Form will be acknowledged. Other **KEY POINTS**: • No PHI may be removed from the VCU ACE under a review preparatory to research • Review Preparatory to Research does not allow for recruitment activities	Allowed identifiers: • Geographic information above the street level (e.g., city, state, zip code) • All elements of dates, including ages over 89 • Other unique identifiers not on the list of 18 HIPAA identifiers Submit a HIPAA data use agreement to the HRPP. HRPP will sign and return a copy to the researcher	Submit a Research on Decedents form to HRPP in REDCap HRPP will review the form and acknowledge the use Other **KEY POINTS** • No IRB review is required if the research only uses decedent data • HRPP has the right to request documentation that all individuals are deceased	Research authorizations require specific information and statements (see templates) Submit with IRB application: 1. Informed Consent document containing Authorization information and statements; OR 2. Separate authorization document in addition to Informed Consent	Submit request to waive authorization with IRB application explaining whether the partial waiver is for recruitment or to waive elements of consent IRB will review and approve justification in smartform	Submit request for waiver of authorization with IRB application IRB will review and approve justification in smartform VCU IRB approval of a waiver may or may not be accepted by other covered providers outside of the VCU ACE