

Learners' Access to PHI

VCU Health System Authority and Affiliates Policy

Owner: Chief Compliance & Privacy Officer

Effective Date: 03/11/2025

Revision: 1.0

This policy applies to Virginia Commonwealth University Health System Authority and all of its wholly owned or controlled affiliates (collectively referred to herein as VCUHS or VCU Health System).

This policy applies to the facilities marked below:

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> VCU Medical Center | <input checked="" type="checkbox"/> Community Memorial Hospital | <input checked="" type="checkbox"/> VCU Health Children's Services at Brook Road |
| <input checked="" type="checkbox"/> VCU Health Ambulatory Surgery Center L.L.C | <input checked="" type="checkbox"/> Community Memorial Hospital (Hundley Center) | <input checked="" type="checkbox"/> VCU Health Tappahannock Hospital |
| <input checked="" type="checkbox"/> MCV Associated Physicians d/b/a MCV Physicians | <input checked="" type="checkbox"/> CMH Physician Services, LLC | |
-

General Information

Resources:

VCUHS Compliance Services	complianceservices@vcuhealth.org
Health Information Management	him@vcuhealth.org

Background

The VCU Health System (VCUHS) is committed to ensuring the privacy and security of Protected Health Information (PHI) in compliance with HIPAA regulations. This policy centralizes the current guidelines for all affiliated student learner groups on accessing and using PHI during their educational, clinical, research, and quality improvement activities.

Purpose

To provide guidance and establish clear expectations for all student learner groups regarding the appropriate use and disclosure of PHI, ensuring compliance with HIPAA and institutional policies.

Definitions

Term	Definition
Clinical Purpose	Activities related to the diagnosis, treatment, and care of patients.

Curated Data Set	Health System Data extracted and transformed by Honest Broker to provide to an Investigator in accordance with institutional policy.
Data Curation	Access to Health System Data to extract and transform Health System Data for research purposes. Data Curation includes, but is not limited to, access to PHI to create De-Identified Data, Limited Data Sets, and other Curated Data Sets for research purposes.
De-Identification	The removal of all identifiers such that there is no reasonable basis to believe that the information can be used to identify an individual or the relatives, employers, or household members of the individual.
Honest Broker	A neutral third-party, who is not part of the team for a particular research study (i.e., is not one of the investigators, study coordinators, statisticians, or data analysts on a research study), that conducts Data Curation for research purposes in accordance with institutional policy. An Honest Broker for a study may not be a co-author on any publication for that same study.
Learner	Any student engaged in a health-related educational program. This includes, but is not limited to, students from accredited medical schools, nursing programs, respiratory therapy, physical therapy, occupational therapy, speech therapy, and other allied health disciplines. Additionally, advanced practice students are also considered learners (e.g., Nurse Practitioners, Nurse Midwives, Clinical Nurse Specialists, and Physician Assistants).
Limited Data Set	Protected health information that excludes specified direct identifiers of the individual or of relatives, employers or household members of the individual.
Minimum Necessary Standard	When using or disclosing PHI, or when requesting PHI, team members must limit the PHI used, disclosed or requested to the least amount reasonably necessary to achieve the purpose of the requested use or disclosure.
Protected Health Information	Protected Health Information (PHI) is individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to: <ol style="list-style-type: none"> 1. Past, present, or future physical or mental health, or condition of an individual; 2. Provision of health care to an individual; or 3. Payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can

	be used to identify an individual, it is considered individually identifiable health information (See Part II, 45 CFR 164.501).
Quality Improvement	Consists of systematic and continuous actions that lead to measurable improvement in health care services and the health status of targeted patient groups.
Research	A systematic investigation designed to develop or contribute to generalizable knowledge.

Policy

- A. It is mandatory that all learners complete mandatory HIPAA training before accessing PHI. This training covers the HIPAA Privacy and Security Rules, including allowable uses and disclosures of PHI, patient rights, and safeguarding PHI.
- B. Learners are permitted to access PHI only when necessary to fulfill their educational, clinical, research, or quality improvement objectives. Learners' PHI access is within approved methods/channels established by the health system (e.g., Epic) and is used solely for specified purposes.
- C. Learners adhere to the Minimum Necessary policy and standard, accessing the information required to complete their educational, clinical, research or quality improvement objectives.
- D. De-identification of VCUHS PHI is approved by Compliance Services or as required by the Research Honest Broker policy.
- E. Learners ensure the integrity, safety and confidentiality of the PHI they access as required by VCUHS policy and by federal regulation.

Procedure

1. Training and Compliance

- 1.1. All learners complete mandatory HIPAA training before accessing PHI.
 - 1.1.1. This training covers the HIPAA Privacy and Security Rules, including allowable uses and disclosures of PHI, patient rights, and safeguarding PHI.
 - 1.1.2. Learners must sign an acknowledgment form confirming their understanding of HIPAA requirements and their commitment to comply with them.
- 1.2. Any documentation of completed training must be maintained by the institution providing.
 - 1.2.1. If learners are participating through an affiliation agreement and receive HIPAA training from their home institution, documentation of that training is provided for review.
 - 1.2.2. Records of training completion are audited, in conjunction with the respective learner program, to ensure compliance.

1.2.2.1. VCUHS maintains documentation in accordance with the record retention standards.

1.3. Annual compliance training courses are updated with any changes in HIPAA regulation and institutional policies.

2. Access to PHI

2.1. Learners are permitted to access PHI only when necessary to fulfill their educational, clinical, research, or quality improvement objectives.

2.2. Access to PHI must be within approved methods/channels established by the health system (e.g., Epic).

2.3. System access granted to learners must be used solely for the specified purposes and not for any other activities.

3. Minimum Necessary Standard

3.1 Learners must adhere to the Minimum Necessary policy and standard, accessing only the information required to complete their educational, clinical, research, or quality improvement objectives.

4. De-identification of PHI

4.1. If VCUHS determines that the de-identification methods are not possible, are impractical, or are excessively burdensome, VCUHS can choose to:

4.1.1. Not release the PHI;

4.1.2. Consider use of a Limited Data Set; or

4.1.3. Guide the requestor of the proper pathway to seek patient authorization for the use and disclosure of their PHI that has not been de-identified.

4.2. De-identified information does not include any patient identifiers as defined by HIPAA. The 18 identifiers are:

4.2.1. Names;

4.2.2. All geographical subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geo-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: (1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000;

4.2.3. 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;

4.2.4. Phone numbers;

4.2.5. Fax numbers;

- 4.2.6. Electronic mail addresses;
- 4.2.7. Social Security numbers;
- 4.2.8. Medical record numbers;
- 4.2.9. Health plan beneficiary numbers;
- 4.2.10. Account numbers;
- 4.2.11. Certificate/license numbers;
- 4.2.12. Vehicle identifiers and serial numbers, including license plate numbers;
- 4.2.13. Device identifiers and serial numbers;
- 4.2.14. Web Universal Resource Locators (URLs);
- 4.2.15. Internet Protocol (IP) address numbers;
- 4.2.16. Biometric identifiers, including finger and voice prints;
- 4.2.17. Full face photographic images and any comparable images; and
- 4.2.18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).

5. Security Measures

- 5.1. Each learner approved for access is assigned unique log-in credentials. The credentials are used for identifying and tracking user identity and access to information systems. Learners must ensure the integrity and confidentiality of PHI that they access. These credentials must be adequately safeguarded and not be disclosed to or shared with any other individual.
- 5.2. Learners must protect the privacy and security of PHI accessed in any clinical setting. This includes not leaving patient files unattended in public areas and following the clinic's specific rules. Additionally, students must ensure that any physical documents containing PHI are securely stored when not in use.
- 5.3. All communication containing PHI must be transmitted through VCUHS approved and secure channels, such as EHR communication tools, VCUHS licensed Microsoft applications, or VCUHS paging systems/applications. Use of non-secure channels, such as SMS, iMessage or other non-secure channels is prohibited to communicate PHI.
- 5.4. Learners will ensure the protection and safeguarding of paper and electronic media containing PHI located on desks, printers, fax machines, photocopy machines, and common areas.
- 5.5. Files and documents containing PHI must be stored in secure locations, such as locked cabinets or encrypted digital storage. Access to these files should be restricted to authorized individuals only.

6. Prohibited Activities

- 6.1. Accessing PHI without proper authorization or a legitimate need to know is strictly prohibited. Unauthorized access can lead to disciplinary actions, including program termination.

- 6.2. Downloading PHI to personal devices, such as laptops, smartphones, or tablets, is not allowed. Similarly, transferring PHI to non-VCUHS managed email accounts or non-VCUHS approved cloud storage services is strictly prohibited. All data transfers must be conducted using secure, encrypted methods approved by VCUHS to ensure the protection of sensitive information.
- 6.3. Sharing PHI with individuals who are not authorized to receive it, including colleagues, friends, or family members, is strictly forbidden. PHI must only be shared with individuals who have a legitimate need to know and are authorized to access the information as part of their job responsibilities.
- 6.4. Improper disposal of PHI, such as discarding documents containing sensitive information in regular trash bins, is prohibited. All PHI must be disposed of securely, following VCUHS guidelines for shredding, de-identification, or other approved methods of destruction.

Privacy Violations: Non-compliance with this policy will result in disciplinary action, which may include termination of access privileges, consequences determined by the learner's enrolled program, and potential legal action. All violations must be reported to the appropriate authorities within the institution.

Related Documents

Policies are available from the list on top right in shaded areas.

Document Type:	Document Name:
VCUHS Authority & Affiliates Policy	PHI Uses and Disclosure for Research Policy
VCUHS Authority & Affiliates Policy	PHI, Administrative, Technical, and Physical Safeguards Policy
VCUHS Authority & Affiliates Policy	De-Identification of PHI Policy
VCUHS Authority & Affiliates Policy	PHI, Minimum Necessary Uses and Disclosures Policy

Evidence Citations

- HIPAA Privacy Rule. Accessed at: <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html#:~:text=The%20HIPAA%20Privacy%20Rule%20establishes,Health%20Care%20Privacy%20%2D%20Final%20Rule>
- [Use and Disclosure of PHI for Training Health Care Professionals - University of Nebraska Medical Center.](#)
- [HIPAA Overview for Clinical Students – Health Insurance Portability and Accountability Act \(HIPAA\)](#)
- [Uses and Disclosures of Protected Health Information for Education and Training - UW-Madison Policy Library](#)