



INSTITUTIONAL POLICY: GA-32

Category: General Administration
Subject: Information Security and Privacy
Effective Date: September 26, 2025
Last Revision Date: N/A

GA 32-1. Authority

1.1 W. Va. Code § 18B-1-6

GA 32-2. Scope

This policy covers the following topics:

- Policy Statement
- Purpose
- Information Security and Privacy Procedures
- Definitions
- Enforceability/Violations
- Implementation of Policy
- References

GA 32-3. Policy Statement

- 3.1 The West Virginia School of Osteopathic Medicine (“WVSOM”), through contractual research agreements with health care facilities and other covered entities, may have access to or come to possess certain sensitive and confidential information, including Protected Health Information. The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH”), and their implementing regulations, as amended, protect such information and prohibit its unauthorized access, use, or disclosure.
- 3.2 This policy shall be applicable to any WVSOM employee, student, volunteer, or others (“Researchers”) who, through participation in approved Research Projects, shall have access to and/or use of Protected Health Information. This policy shall also apply to any clinical faculty (“Clinical Faculty”) who, through their clinical duties at other Covered Entities, including, but not limited to, the Robert C. Byrd Clinic, may have access to and/or use of Protected Health Information. WVSOM, its Researchers, and Clinical Faculty and any other employee or student authorized to access PHI shall protect such information as required by HIPAA, HITECH, their implementing regulations as amended, this policy, and applicable WVSOM procedures. WVSOM is not a Covered Entity, does not provide health care services, and no department or program functions as a Covered Entity or health care facility. Further, WVSOM is not a Business Associate of any Covered Entity, and does not perform

any functions on behalf of any Covered Entity. As WVSOM is neither a Covered Entity nor a Business Associate, WVSOM, as an organization, is not subject to HIPAA; however, Researchers, Clinical Faculty, and any other employee or student authorized to access PHI must follow this policy and all applicable HIPAA regulations.

GA 32-4. Purpose

The purpose of this policy and the procedures listed in Section 5.1 is to:

- 4.1 Protect WVSOM's information and system resources.
- 4.2 Help to ensure the confidentiality, integrity, and availability of information assets that may contain or transmit electronic Protected Health Information.
- 4.3 Establish an information security and privacy policy management and governance structure.
- 4.4 Create awareness for the Researchers and Clinical Faculty in making information security decisions in accordance with this policy and applicable WVSOM procedures.
- 4.5 Help protect sensitive and confidential information from unauthorized use, disclosure, modification, or destruction as required by HIPAA, HITECH, and their implementing regulations.
- 4.6 Provide direction to those responsible for the design, implementation, and maintenance of systems that support WVSOM's operations.
- 4.7 Clarify management and other responsibilities and duties with respect to the protection of information assets and resources.
- 4.8 Support compliance with HIPAA, HITECH, their applicable regulations, as amended, and other applicable legal and regulatory requirements.

GA 32-5. Information Security and Privacy Procedures

- 5.1 WVSOM shall implement and maintain procedures to support this policy which set forth security and privacy requirements for all WVSOM Researchers, Clinical Faculty, or any other employee or student authorized to have access to PHI or that create, maintain, store, access, process, or transmit information. Those procedures address the following categories:
 - 5.1.1 HIPAA Information Security and Privacy Program
 - 5.1.2 Security and Privacy Management Process
 - 5.1.3 Awareness and Training
 - 5.1.4 Facility Access, Network/Data Transmission, and Storage Safeguard
 - 5.1.5 Security Incident and Privacy Breach Response

- 5.2 This policy and supporting procedures apply to all of WVSOM's Researchers, Clinical Faculty, and any other student or employee given authorization to access PHI, generally under an approved Research Project. Prior to accessing any PHI, Researchers and Clinical Faculty, or any others who may access PHI, shall sign a confidentiality agreement which states that they 1) have read this policy and accompanying procedures; 2) have participated in HIPAA training and awareness; 3) understand and acknowledge their obligations with respect to access, use, storage, and disclosure of PHI; 4) agree to access PHI only and exclusively through HIPAA-compliant Access Software; and 5) agree to promptly report any breach of PHI using the appropriate forms as approved by WVSOM.
- 5.3 This policy and supporting procedures pertain to all WVSOM systems, applications and information in all forms in all locations where WVSOM business processes are performed.
- 5.4 This policy and supporting procedures cover WVSOM's network system which is comprised of various hardware, software, communication equipment and other devices designed to assist WVSOM in the creation, receipt, storage, processing, and transmission of information. This includes equipment connected to any WVSOM domain or Virtual Local Area Networks ("VLAN"), either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by WVSOM at its office locations or at remote locales, and the personally-owned computing devices used for WVSOM purposes.

GA 32-6. Definitions

The following terms as used throughout this policy and supporting procedures shall have the meanings as set forth in this section.

- 6.1 "Access Software" means a software program that includes secure remote access, cloud storage, secure messaging, and/or electronic signature solutions designed to be compliant with applicable HIPAA regulations and to protect the privacy and confidentiality of PHI. Features, updates, and HIPAA compliance are the responsibility of the vendor which owns and/or operates the Access Software.
- 6.2 "Breach" means the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The term "Breach" does not include any unintentional acquisition, access, or use of Protected Health Information by WVSOM student or employee if:
 - 6.2.1 such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship with WVSOM; and such information is not further used or disclosed in an unauthorized manner; or
 - 6.2.2 any inadvertent disclosure by a person who is authorized to access Protected Health Information to another person with the same authorization; and the information received as a result of such disclosure is not further used or disclosed in an unauthorized manner; or

- 6.2.3 the disclosure of Protected Health Information where WVSOM has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- 6.3 “Business Associate” means a person or entity that creates, receives, maintains, or transmits Protected Health Information on behalf of a Covered Entity as described in § 164.308(b) of the Security Rule and § 164.502(e) of the Privacy Rule, but other than in the capacity of a member of the workforce of such Covered Entity.
- 6.4 “Clinical Faculty” means a WVSOM employee who is considered a member of the faculty, and who, through their employment agreement with WVSOM, is authorized to and is actively practicing medicine at a Covered Entity, which includes, but is not limited to, the Robert C. Byrd Clinic, and who may be authorized to access PHI of their current or former patients, in their role as a physician for such Covered Entity.
- 6.5 “Electronic Protected Health Information” or “EPHI” means Protected Health Information in any type of electronic form.
- 6.6 “Health Information Technology” or “HIT” means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information.
- 6.7 “Individually Identifiable Health Information” or “IIHI” has the same meaning as Protected Health Information.
- 6.8 “Information Security” means the preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
- 6.9 “Protected Health Information” or “PHI” means Individually Identifiable Health Information:
- 6.9.1 That is:
- a. Transmitted by or maintained in electronic media; or
 - b. Transmitted by or maintained in any other form or medium.
- 6.9.2 PHI excludes Individually Identifiable Health Information in:
- a. Education Records as defined by the Family Educational Rights and Privacy Act.
 - b. Records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student’s choice.

- c. Employment records held by an entity in its role as employer.
 - d. Records regarding a person who has been deceased for more than 50 years.
- 6.9.3 PHI is information that is a subset of health information, including demographic information collected from an individual, and:
- a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
 - b. 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
 - i. That identifies the individual; or
 - ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- 6.9.4 The explicitly identified PHI items are set forth as follows:
- a. Names
 - b. Addresses
 - c. Geographic subdivisions smaller than a state
 - d. All elements of dates directly related to the individual (dates of birth, marriage, death, dates of service, etc.)
 - e. Telephone numbers
 - f. Facsimile numbers
 - g. Driver's license numbers
 - h. Electronic mail addresses
 - i. Social security numbers
 - j. Medical record numbers
 - k. Health plan beneficiary numbers
 - l. Account numbers, certificate/license numbers
 - m. Vehicle identifiers and serial numbers
 - n. Device identifiers and serial numbers
 - o. Web Universal Resource Locators (URLs)
 - p. Internet Protocol (IP) address numbers
 - q. Biometric identifiers
 - r. Full face photographic images and any comparable images
 - s. Genetic data that is individually unique

- 6.10 “Personally Identifiable Information” or “PII” means any piece of information, or combination of information items, that can be associated with one individual. PII items are typically considered to be those explicitly specified with any one of a number of data protection and privacy laws.
- 6.11 “Personal Information” means information that can be linked to a specific individual, group of individuals, or reveal activities or other types of characteristics of an individual or group. Many types of Personal Information are not explicitly protected by any law or regulation. PII is a subset of Personal Information.
- 6.12 “Qualified Electronic Health Record” means an electronic record of health-related information on an individual that:
- 6.12.1 includes patient demographic and clinical health information, such as medical history and problem lists; and
 - 6.12.2 has the capacity to:
 - a. provide clinical decision support;
 - b. support physician order entry;
 - c. capture and query information relevant to health care quality; and
 - d. exchange electronic health information with, and integrate such information from, other sources.
- 6.13 “Research Project” means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge, and that has been approved by WVSOM’s Office of Research and Sponsored Programs (“ORSP”), through applicable policies and procedures.
- 6.14 “Researcher” means employees, volunteers, students, trainees, and other persons who, through performing research-related or research support duties under an approved Research Project, may have access to or use of Protected Health Information.

GA 32-7. Research Projects

- 7.1 In the course of a Research Project, Researchers may obtain, create, use and/or disclose PHI. Unless the PHI has been de-identified by the Covered Entity prior to permitting WVSOM’s Researchers access, WVSOM must obtain one of the following, in conjunction with the Research Project:
- 7.1.1 Individual authorization of PHI for research purposes, in which each individual whose PHI is to be disclosed for use in research must sign a waiver of authorization, originating with the Covered Entity, that meets all applicable requirements of the HIPAA Privacy Rule; or
 - 7.1.2 Approval from WVSOM’s Institutional Review Board (“IRB”) to proceed with a Research Project under a waiver of authorization of those individuals whose PHI is to be disclosed for use in research. This approval is generally for those Research Projects that are unable to use de-identified PHI, and when the research could not

practically be conducted if individual authorization was required. Such approval must include: 1) date of approval and identification of the IRB; 2) a statement that the IRB has determined the waiver of authorization satisfies the criteria of the Privacy Rule, and has been reviewed under normal and applicable review procedures; 3) a brief description of the PHI for which access has been determined to be necessary by the IRB; and 4) signature of the IRB Chair.

GA 32-8. Enforceability/Violations

Any Researcher or Clinical Faculty who violates this policy or procedures may be subject to disciplinary action up to and including termination of employment, termination of contract, or dismissal from school, as applicable.

GA 32-9. Implementation of Policy

This policy will be implemented using applicable WVSOM policies and procedures and WVSOM faculty, employee, and student handbooks.

GA 32-10. References

- 10.1 HIPAA, 45 C.F.R. § 164.306, Security Standards: General Rules
- 10.2 HIPAA, 45 C.F.R. § 164.501, 164.508, 164.512(i), Research
- 10.3 NIST SP 800-66
- 10.4 NIST SP 800-37
- 10.5 NIST SP 800-53
- 10.6 ISO/IEC 27001: A.5 Security Policy
- 10.7 ISO/IEC 27002: 2005 Section 5: Security Policy