WASHINGTON STATE UNIVERSITY
Elson S. Floyd
College of Medicine

Policy Title: HIPAA Training for Faculty and Students

Policy Number: EC.00.07.200414

Applies to: All WSU Elson S. Floyd College of Medicine Faculty and Students

Date: 10/12/2023

**1.0 Policy Statement:**

It is WSU College of Medicine's policy that the College of Medicine provides training to faculty and students on HIPAA to protect the confidentiality, integrity, and availability of protected health information (PHI).

1.1 The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted.

1.2 When personally identifiable information is used in conjunction with one's physical or mental health or condition, health care, it becomes protected health information (PHI).

1.3 In accordance with the HIPAA Privacy Rule, the College of Medicine trains faculty and students at an appropriate level to fulfill their roles and responsibilities.

1.4 The College of Medicine provides faculty and students training specific to their job responsibilities. Administrators who oversee operations that create or may use PHI receive HIPAA training to help assure compliance with faculty and students as necessary and appropriate for them to carry out their responsibilities.

1.5 In accordance with the HIPAA privacy rule, there are 18 HIPAA identifiers that are considered personally identifiable information. This information can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual.

**2.0 Definitions**

*De-Identification:* De-identification is the action of removing all patient identifiers that

can be linked to any individual or re-identified**.** The action mitigates privacy risks to individuals and thereby supports the secondary use of data for comparative effectiveness studies, educational purposes, policy assessment, life sciences research, and other endeavors.

*HIPAA:* The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy, and security of health information.

*Minimum Necessary Rule:* The minimum necessary standard is the key protections of the HIPAA Privacy Rule. Protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires evaluation of practices and enhance safeguards as needed to limit unnecessary or inappropriate

access to and disclosure of protected health information.

*Protected Health Information (PHI)*: Information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 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; that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

*Washington's Uniform Health Care Information Act, RCW 70.02:* Washington's state law that governs the use, access, and disclosure of patients' health care information, whether oral or recorded in any form or medium. The law applies to licensed health care providers, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider. See RCW 70.02.020.

## 3.0 Responsibility

Office of Compliance

## 4.0 Procedures

**HIPAA Training for Faculty**

College faculty receive training in HIPAA commensurate with their academic role. Training is provided by WSU and monitored by the Office of Compliance in coordination with Office of Faculty Development in alignment with the Office of Inspector General's recommendations for HIPAA training.

**HIPAA Training for Administrators**

College administrators who oversee operations that create or may use PHI receive training in HIPAA commensurate with their organizational role. The Office of Faculty Development provides training and monitoring in alignment with the Office of Inspector General's recommendations for HIPAA training.

**HIPAA Training for Students**

All students in the College of Medicine participate in HIPAA training appropriate to their level of matriculation in the curriculum. The Office of Curriculum provides training and monitoring in alignment with the Office of Inspector General's recommendations for HIPAA training prior to entry into residency.

**HIPAA Attestation**

Clinical faculty attests to completing HIPAA training at the healthcare organization where they work as healthcare providers. WSU COM acquires attestation from clinical faculty annually. The Office of Compliance monitors, stores and audits attestation documentation.

**Graduate Medical Education (GME)**

The Department of Graduate Medical Education under the direction of the Associate Dean of Graduate Medical Education manages all GME HIPAA training.

**Minimum Necessary Information**

At the College of Medicine, employees, faculty, and students implement ways to minimize breaches. HIPAA Privacy Rule states that PHI should not be used or disclosed when it is not

necessary to satisfy a particular purpose or carry out a function. The PHI used to conduct the education/training must be the minimum necessary needed to accomplish the purpose. All PHI must be de-identified for any purpose, including student assignments. If patient authorization is granted, the minimum necessary PHI is not required. For example, if a patient gives permission to a College of Medicine faculty member for a patient presentation, then PHI can be discussed without being de-identified or meet the minimum necessary rule.

**De-Identification**

College of Medicine faculty and students can use health information that has been de-identified in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. De-identification is the action of removing all identifiers that can be linked to any individual or re-identified. The method that can be used to satisfy the Privacy Rule's de-identification standard is the Safe Harbor Standard. The Safe Harbor Standard is the anonymization of PHI by removing 18 HIPAA identifiers. When these identifiers are removed, the information is no longer considered protected and can be released without harm to the patient.

**Safe Harbor**

The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names

(B) All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits if the 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

(C) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, 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

(D) Telephone numbers

(L) Vehicle identifiers and serial numbers, including license plate numbers

(E) Fax numbers

(M) Device identifiers and serial numbers

(F) Email addresses

(N) Web Universal Resource Locators (URLs)

(G) Social security numbers

(O) Internet Protocol (IP) addresses

(H) Medical record numbers

(P) Biometric identifiers, including finger and voiceprints

(I) Health plan beneficiary numbers

(Q) Full-face photographs and any comparable images

(J) Account numbers

(R) Any other unique identifying number, characteristic, or code

(K) Certificate/license numbers

*(Reference: §164.502(d), §164.514(a-c), Health Insurance Portability and Accountability Act of 1996)*

All students and faculty must practice de-identification. Failure to properly de-identify PHI shall result in HIPAA breaches. These breaches are reportable to the affiliated organization. Records,

including student assignments, with PHI, must not be placed on any electronic system owned by the College of Medicine. Electronic and hard copy forms created by the Department of Student and Faculty Experience used by faculty and students to document patient cases shall be reviewed by the Office of Compliance to ensure PHI is not being collected and inappropriately used.

**Compliance**

The Office of Compliance maintains responsibility for the designation of a compliance contact for all internal auditing and monitoring activities. Students and faculty who have questions or concerns regarding HIPAA should seek out the services of the Office of Compliance

**Records Management**

Documentation of attestation and training documentation of satisfactory completion of HIPAA for students and faculty are kept for six years.

**Reporting**

If any faculty and students are made aware of any actual or alleged violation of HIPAA, RCW 70.02, and/or this Policy, the individual is required to bring to the attention of the Compliance Specialist for reporting the actual or alleged violation.

College of Medicine Office of Compliance
Office Email:
medicine.compliance@wsu.edu
Phone: (509) 368-6511

The Compliance and Civil Rights University French Administration Building, Room 225
Email: crci@wsu.edu
Phone: (509) 335-8288
Fax: (509) 335-5483

Department of Health and Human Services' Office for Civil Rights
Customer Response Center: (800) 368-1019
Fax: (202) 619-3818
TDD: (800) 537-7697
Email: ocrmail@hhs.gov

**Potential Breach or Noncompliance Investigations**:

The College of Medicine Office of Compliance promptly investigates any potential privacy or security incident, or violation of this policy, of which they are notified and recommends appropriate corrective actions in the event that a breach has occurred. The Office of Compliance has the right to involve the WSU and/or the College of Medicine Information Security Office, Office of the General Counsel, or administrative areas as appropriate. In the event any other College of Medicine

department receives the notification of a potential HIPAA violation or violation of this policy, the department promptly notifies the Office of Compliance.

All students and faculty are required to cooperate in such investigations and promptly respond to inquiries from the Office of Compliance and any other such requests from administrative areas assisting with or coordinating the investigation. Failure to cooperate with an investigation concerning a privacy or security breach, or a violation of this policy, may result in disciplinary action by the College of Medicine. The nature of the breach determines the investigative process. (Reference: Business Policy BPPM 88.05)

**Whistleblowing**

College of Medicine faculty and students have the ability to disclose PHI for the purpose of making a whistleblower complaint to health oversight agency, a public health authority authorized to investigate the conduct in question or a healthcare accreditation organization. Intimidation, retaliation, and/or discrimination against any individual for exercising an individual's rights under applicable privacy laws, including, but not limited to, filing a complaint regarding a privacy practice, is strictly prohibited. (Reference: Business Policy BPPM 10.20)

**Consequences**

Violations of this policy regarding state and federal law result in disciplinary action and/or other corrective methods. Investigations and determinations regarding corrective measures are made in accordance with the College of Medicine's existing policies and procedures. Anyone in violation of this policy may be subject to corrective action under the applicable policies and procedures. Individuals who violate HIPAA regulations may be subject to civil and criminal penalties as provided by state and federal law. (Reference: Business Policy BPPM 60.50)

## 5.0 Related Policies

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Washington's Uniform Health Care Information Act, RCW 70.02
WSU EP Chapter 88 – Information Privacy
WSU EP #4 - Electronic Communication Policy
WSU EP #8 - University Data Policies
WSU EP #37 - Information Security Policy

## 6.0 Key Search Words

Protected Health Information, Health Insurance Portability, and Accountability Act, Training

## 7.0 Revision/Review of History

Original Approval Policy number 4/20/2020 EC.00.07.200414
Review/Revision 4/14/2020