Elson S. Floyd College of Medicine
WASHINGTON STATE UNIVERSITY

Policy Title: Research HIPAA Policy

Policy Number: EC.00.08.200922

Applies to: All WSU Elson S. Floyd College of Medicine investigators involved in College of Medicine human subject research.

Date: 09/22/2020

1.0 Policy Statement:

It is the WSU College of Medicine's policy that College of Medicine investigators involved in human subject research protect the confidentiality, integrity, and availability of protected health information (PHI).

2.0 **Definitions**

Authorization: is a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the individual.

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.

Federal Policy for the Protection of Human Subjects: also known as the "Common Rule," governs the ethical conduct of research involving human subjects. Fifteen federal agencies and departments are party to this rule, which first came into effect in 1981. See 45 CFR § 46.

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 US Department of Health and Human Services (HHS) to publicize standards for the electronic exchange, privacy, and security of health information.

HIPAA 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.

HIPAA Security Rule: requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI (ePHI).

Investigators: Individuals performing various tasks related to the conduct of human subject research activities, such as obtaining informed consent from subjects, interacting with subjects, and communicating with an Institutional Review Board (IRB). Investigators include College of Medicine faculty, students, staff, and administration.

Human Subject: A living individual about whom an investigator (whether professional or student) conducting research:

(i). Obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or

(ii) Obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens. *See* 45 CFR § 46.102.

***Protected Health Information (PHI)*:** is 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 concerning which there is a reasonable basis to believe the information can identify the individual. *See* 45 CFR § 160.103.

Limited Data Set: is PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's authorization or a waiver or an alteration of authorization for its use and disclosure, with a data use agreement. *See* 45 CFR § 164.514(e).

Personal Identifiable Information (PII): is the information used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

3.0 Responsibility

Elson S. Floyd College of Medicine Compliance Specialist

4.0 Procedures

The WSU Office of Research Assurances (ORA) educates and trains WSU faculty and students, at an appropriate level, to fulfill their roles and responsibilities with safeguarding PHI and/or other individually identifying information (e.g., personal information, health care information, personal records) used in approved research. This education and training occur before investigators conduct research, and it includes applicable federal (e.g., HIPAA) and state privacy and security laws.

HIPAA Training for Investigators

The WSU Office of Research Assurances provides appropriate training to investigators in alignment with the HHS recommendations for HIPAA training through the Collaborative Institutional Training Initiative (CITI) before engaging in human subject research.

HIPAA Privacy Rule

The HIPAA Privacy Rule sets forth standards to protect all PHI that is maintained, accessed, or disclosed. These are the 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.

Authorization

Generally, the HIPAA Privacy Rule requires written authorization from human subject participants before investigators may use or disclose the individual's PHI. The HIPAA requirements for authorization are additional to the informed consent regulations of the Food and Drug Administration (FDA) and the HHS. Under specific circumstances,

however, the HIPAA Privacy Rule permits an investigator to use or disclose PHI for research without an individual's authorization. College of Medicine Investigators may only use or disclose PHI without an individual's authorization by obtaining the proper waiver of authorization documentation required by the WSU Institutional Review Board (IRB).

De-Identification

Investigators within the College of Medicine may use health information that has been de-identified in accordance with the HIPAA Privacy Rule. De-identification is the action of removing all identifiers that can be linked to any individual or re-identified. When these identifiers are removed, the information is no longer considered PHI and can be released without harm to the individual.

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

(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 of 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

And the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(Reference: 45 CFR §164.502(d), 45 CFR §164.514(a-c), Health Insurance Portability and Accountability Act of 1996)

College of Medicine investigators may use Limited Data Sets for research purposes without obtaining an individual's authorization or a waiver with a data use agreement. The data use agreement must meet the regulatory requirements and establish how the PHI in the Limited Data Set may be used and how it will be protected. PHI in Limited Data Sets may include city, state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed in the regulation as direct identifiers.

Institutional Review Board

WSU engages in human subject research and is required to designate an IRB in support of compliance with federal laws and regulations. WSU IRB has the authority to approve, require modification, or reject all research activities covered by the HHS and FDA, protection of human subject regulations, including HIPAA. At WSU, the IRB is the acting HIPAA Privacy Board. All College of Medicine Investigators must comply with WSU IRB standards and must receive IRB approval before starting research. Following approval, College of Medicine investigators must comply with all WSU IRB requirements, including periodic reviews.

HIPAA Security Rule

Investigators within the College of Medicine must use appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI. The College of Medicine Office of Research in collaboration with WSU Information Technology (IT) and ORA must implement and monitor the performance of the security management process, assignment or delegation of security responsibility, training requirements, and evaluation and documentation of all decisions regarding PHI. Assurances must implement and monitor the performance of the security management process, assignment or delegation of security responsibility, training requirements, and evaluation and documentation of all decisions regarding PHI.

Administrative Safeguards

Investigators must follow WSU regulations for access and use of PHI. Behavioral safeguards monitor the conduct of investigators for the protection of PHI. Only Investigators that have completed CITI training can manage PHI through a secure HIPAA compliant electronic data management information system. WSU IRB and WSU IT monitors and maintains the management of PHI for potential breaches.

Physical Safeguards

HIPAA Security Rule sets forth standards for physical measures to protect PHI and HIPAA compliant information systems and equipment, and related offices and buildings from unauthorized access and environmental threats. Investigators must adhere to physical safeguards as appropriate in any physical location where PHI is maintained and/or accessed.

Technical Safeguards

Investigators are to refer to WSU Executive Policy #37, WSU Executive Policy #8, WSU BPPM #45.35, and Human Research Protection Program (HRPP) Office's guidance on securing human subject research data. For data storage and management, human subject investigators must use WSU Amazon Web Services (AWS), or an equivalent solution determined by the WSU Chief Information Officer or the WSU Chief Information Security Officer. Human subject investigators must not retain any PHI on any personal devices or unsecured electronic media, including mobile devices (e.g., USB drives, CDs, laptops). Failure to properly store PHI may result in HIPAA breaches, which must be reported in

accordance with the law to appropriate government agencies, affiliated organizations, and/or the individual.

Reporting
All investigators are responsible for reporting potential breaches or noncompliance events when they learn of them to the Elson S. Floyd College of Medicine Vice Dean for Research and the College of Medicine Compliance Specialist. The College of Medicine Vice Dean for Research shall report any potential breach or noncompliance event to WSU's Chief Information Security Officer (CISO) and Chief Compliance and Risk Officer (CCRO). The CISO and CCRO will determine if an investigation is necessary and determine whether the incident must be reported to outside entities, which may include sponsors and other regulatory bodies, and initiate any required reporting.

Potential Breach or Noncompliance Investigations
Investigations and determinations regarding corrective measures are made in accordance with WSU policies.

Reporting Compliance Concerns
College of Medicine investigators may disclose the minimum necessary PHI for the purpose of reporting a compliance concern to an appropriate oversight agency or public health authority in accordance with the law. Reporters should generally use de-identified data to the greatest extent possible when reporting a compliance concern. College of Medicine investigators may also disclose de-identified data to appropriate WSU officials charged with receiving compliance concerns on behalf of the institution. Disclosures of data shall be in accordance with all applicable laws, and WSU policy. Intimidation, retaliation, and/or discrimination against an individual for filing a good faith compliance concern is strictly prohibited.

Consequences
Violations of this policy, and/or state and federal law may result in disciplinary action and/or other corrective actions in accordance with WSU policy. Individuals who violate laws applicable to safeguarding regulated data (e.g., HIPAA) may also be subject to civil and criminal penalties as provided by state and federal law.

5.0 Related Policies

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Federal Policy for the Protection of Human Subjects, 45 CFR part 46
Washington's Uniform Health Care Information Act, RCW 70.02
Release of Records for Research, RCW 42.48
WSU EP #4 - Electronic Communication Policy
WSU EP #8 - University Data Policies
WSU EP #37 - Information Security Policy
WSU BPPM #45.35 Managing Research Records
EC.00.07.200414- HIPAA Training for Faculty and Students

6.0 Key Search Words

Protected Health Information, Privacy, Security, Health Insurance Portability and Accountability Act, IRB, Human Subject Research

7.0 Revision/Review History

Date of Original Approval	Policy number	Review/Revision
09/22/2020	EC.00.08.200922	

Responsible Offices: Office of Compliance coordinating with the College of Medicine Office of Research

Policy Contact: Compliance Specialist

Supersedes: N/A