WASHINGTON STATE UNIVERSITY
Elson S. Floyd
College of Medicine

Policy Title: Range Community Clinic – Speech-Language Pathology Services HIPAA and Privacy

Policy Number: EC.00.06.200414

Applies to: WSU Elson S. Floyd College of Medicine faculty, staff, and students participating in the WSU Speech-Language Pathology Services under Range Community Clinic (SLPS-RCC)

Date: 08/01/2023

1.0 Policy Statement

Washington State University's Elson S. Floyd College of Medicine (COM) policy maintain that faculty, staff, and students assigned to or involved with the SLPS-RCC protect the confidentiality, integrity, and availability of protected health information (PHI) and health care information in accordance with the SLPS-RCC's privacy/security policies, and federal and state laws.

2.0 Definitions

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.

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.

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 concerning which there is a reasonable basis to believe the information can to identify the individual. See 45 CFR § 160.103.

Minimum Necessary Information: The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted. These are the 18 HIPAA Identifiers that are considered personally identifiable information. (See section 1.1.4) 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. When personally identifiable information is used in conjunction with one's physical or mental health or condition, healthcare, it becomes protected health information (PHI). 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 presentation of case report, then PHI can be discussed without being de-identified or meet the minimum necessary rule. Case report is the detailed description of patient's conditions, diagnosis, treatment, and follow-up used for a purpose with educational value by health care providers.

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 18 HIPAA 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 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

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

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 Speech Language Pathology Services (Speech and Hearing Sciences 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.

Workforce Member: Range Community Clinic is an affiliate of Speech Language Pathology Services (Speech and Hearing Sciences), WSU College of Medicine faculty, who are licensed and certified health care providers, render health care services for the Range Community Clinic's patients and provide supervision and educational direction to WSU College of Medicine students.

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.

Compliance: The WSU 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.

3.0 Responsibilities

Office of Compliance

4.0 Procedures

Verification

WSU College of Medicine faculty, staff, and students participating in the Range Community Clinic must adhere to any Clinic privacy and security policies and undertake and complete any compliance education provided by the Clinic. WSU College of Medicine faculty, staff, and students are required to complete and sign privacy, confidentiality, and data security agreements and complete annual HIPAA training. WSU College of Medicine faculty, staff, and students must maintain the confidentiality of the Clinic's PHI and limit the disclosure of PHI in accordance with the Clinic's policy and the law. WSU College of Medicine faculty, staff, and students must not use, access, or disclose PHI without the patient's written authorization unless permitted by law. WSU College of Medicine faculty, staff, and students must undertake and successfully complete basic and specific and/or supplemental clinical HIPAA training appropriate to their role in the clinic's function.

HIPAA Training

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

of Medicine provides participating faculty, staff, and students with annual training regarding HIPAA and state regulatory requirements. Clinic administrators function as a member of the Clinic's workforce and receive HIPAA training to help assure compliance with employees and students as necessary and appropriate for them to carry out their responsibilities at the Clinic. Faculty, staff, and students must complete all necessary and required training. Participating WSU College of Medicine students must undergo data security and privacy (HIPAA) training through WSU College of Medicine's electronic education and document management system.

Monitoring

WSU College of Medicine policy prohibits any maintenance or storage of Clinic related PHI with the WSU College of Medicine or WSU IT or physical environments. Under the HIPAA Security Rule, WSU College of Medicine faculty, staff, and students must comply with all safeguards put in place to protect PHI.

WSU College of Medicine faculty, staff, and students must not have access to PHI in a clinical setting unless they have completed the WSU College of Medicine's HIPAA training. The WSU College of Medicine Office of Compliance must perform all audits of faculty, staff, and student training on an appropriate basis or when otherwise deemed necessary. WSU College of Medicine Students must remain in compliance with this standard to satisfy degree requirements. All documentation of data security and privacy (HIPAA) training for students is managed in CastleBranch and Precipio. The Office of Talent Recognition & Enhancement manages faculty and staff HIPAA training documentation. In accordance with the law, WSU College of Medicine retains training documentation for six years.

Reporting

WSU College of Medicine faculty, staff, and students participating in the Clinic must immediately report any known or suspected security incidents or breaches of PHI to the WSU College of Medicine's Office of Compliance. Disclosure of any known or suspected security incident to the WSU College of Medicine's Office of Compliance should include the disclosure of the PHI involved in the incident. WSU College of Medicine faculty, staff, and students must report any attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI within WSU information system operations. Failure to comply with WSU College of Medicine or Range Community Clinic's HIPAA policies may result in, among other things, appropriate corrective action including termination or appropriate discipline in accordance with WSU policy or loss of your assignment/appointment in the Clinic in accordance with the Clinic's corrective action policy.

WSU College of Medicine Office of Compliance may assist the Range Community Clinic's Privacy Officer where appropriate and necessary in investigating potential or actual privacy or security violations at the Clinic, but only to the extent, there is no exchange or access of PHI. Where appropriate or necessary, the Office of Compliance has the right to involve necessary stakeholders to assist with the investigation, such as the WSU College of Medicine Information Security Office, the Attorney General's Office, or administrative areas as appropriate. Stakeholders will need to be part of WSU's health care component or take all necessary action to comply with HIPAA if there will be access to PHI. In the event any other WSU 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. Any investigations and/or inquiries from Range Community Clinic must be handled promptly by the WSU College of Medicine Office of Compliance.

WSU College of Medicine faculty, staff, and students participating in the Clinic are required to cooperate in such investigations and promptly respond to inquiries from WSU College of Medicine Office of Compliance and to 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 corrective action per the Clinic's policy or discipline in accordance with the WSU College of Medicine policy.

WSU College of Medicine faculty, staff, and students participating in the Clinic may disclose PHI to make a whistleblower complaint to a 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.

Violations of this policy and state and federal law may result in appropriate disciplinary and/or other corrective action. WSU College of Medicine's existing policies and procedures determine corrective measures regarding investigations and determinations. Students in violation of this policy may be subject to disciplinary action under the applicable student policies and procedures. Individuals who violate HIPAA or other privacy laws may be subject to civil and criminal penalties as provided by state and federal law.

5.0 Related Policies

HIPAA Training for Faculty and Students EC.00.07.200414
Title 45 Code of Federal Regulations
RCW 70.02.020
College of Medicine Conflict of Interest Policy EC.01.01.191203
WSU Conduct Code https://conduct.wsu.edu/Title 504 Chapter 26
WSU Ethics, Conflict of Interest and Technology Transfer Policy
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

Range Community Clinic – Speech-Language Services, Protected Health Information, Privacy, Security, Health Insurance Portability and Accountability Act

7.0 Revision History

Original Approval Policy number 4/14/2020 EC.00.06.200414
Review/Revision 04/14/2020 04/14/2020 08/01/2023

WASHINGTON STATE UNIVERSITY
Elson S. Floyd
College of Medicine

Confidentiality Agreement

Department of Speech and Hearing Sciences

As an employee, temporary employee, volunteer, student, or student employee in the Department of Speech and Hearing Sciences at Washington State University, you may have access to what this Agreement refers to as "Confidential Information." The purpose of this Agreement is to help you understand your duty regarding confidential information.

"Confidential information" includes information about employees, clients, research subjects, students, or financial or other business or academic information relating to the Department of Speech and Hearing Sciences at Washington State University. You may learn or have access to confidential information through Range Community Health computer systems.

As an individual having access to confidential information, you are required to conduct yourself in strict conformance with applicable laws and Department of Speech and Hearing Sciences policies governing confidential information. As a condition of your relationship to the Department of Speech and Hearing Sciences, you are required to acknowledge and abide by these duties. A violation of any of these duties will subject you to discipline, which might include, but is not limited to, dismissal of your relationship (e.g., faculty appointment, employment, dismissal from the program (in case of a student), consulting, etc.) with Department of Speech and Hearing Sciences, in addition to legal and/or financial liability.

I understand that I may have access to electronic, printed, or spoken confidential information, which may include, but is not limited to, information relating to:

- Clients/ Patients of Range Community Clinic – including patient names, geographical elements (such as a street address, city, county, or zip code), dates related to the health or identity of individuals (including birthdates, date of admission, date of discharge, date of death, or exact age of a patient older than 89), telephone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health insurance beneficiary numbers, account numbers, certificate/ license numbers, vehicle identifiers, device attributes or serial numbers, digital identifiers, such as website URLs, IP addresses, biometric elements, including finger, retinal, and voiceprints, full face photographic images, other identifying numbers or codes.
- Employees – including salaries, employment records, disciplinary actions, etc.
- Students – including enrollment, grade, and disciplinary information.
- Research – including protected health information (PHI) created, collected, or used for research purposes.
- Department of Speech and Hearing Sciences – including but not limited to financial and statistical records, strategic plans, internal reports, memos, peer review information, communications, proprietary computer programs, source code, proprietary technology, etc.
- Third party information – including computer programs, client and vendor proprietary information, source code, proprietary technology, etc.
- Personal Identifying Information (PII) used in other contexts.

Examples of inappropriate disclosures include:

- Employees discussing or revealing confidential information to friends or family members.
- Employees discussing or revealing confidential information to other employees without a legitimate need to know.

- Using confidential information for marketing purposes without express permission from Department of Speech and Hearing Sciences, employee student, or patient.

The unauthorized disclosure of confidential information by employees can subject each individual employee and the practice to civil and criminal liability. Disclosure of confidential information to unauthorized persons, or unauthorized access to, or misuse, theft, destruction, alteration, or sabotage of such information, is grounds for disciplinary action up to and including termination.

Accordingly, as a condition of, and in consideration of my access to confidential information, I promise that:

1. I will use confidential information only as needed by me to perform my legitimate duties as defined by my relationship (faculty, employment, student, visitor, consulting, etc.) with the Department of Speech and Hearing Sciences.
    - I will not access confidential information, which I have no legitimate need to know.
    - I will not in any way divulge copy, release, alter, revise, or destroy any confidential information except as properly authorized within the scope of my relationship with the Department of Speech and Hearing Sciences.
    - I will not misuse or carelessly handle confidential information.
    - I understand that it is my responsibility to assure that confidential information in my possession is maintained in a physically secure environment.
2. I will safeguard and will not disclose to any other person my password or any other authorization code that allows me access to confidential information. I will be responsible for misuse or wrongful disclosure of confidential information that may arise from sharing access codes with another person and/or for failure appropriately to safeguard my password or other authorization to access confidential information.
3. I will log off computer systems after use.
4. I will not log on to a system or access confidential information to allow another person access to that information or to use that system.
5. I will report any suspicion or knowledge that my access code, authorization, or any confidential information has been misused or disclosed without the authorization of the Department of Speech and Hearing Sciences or Range Community Clinic.
6. I will not download or transfer computer files containing confidential information to any non-authorized computer of the Department of Speech and Hearing Sciences or Range Community Clinic, data storage device, portable device, telephone, or other device capable of storing digitized data.
7. I will only print documents containing confidential information in a physically secure environment, will not allow other persons' access to printed confidential information, will store all printed confidential information in a physically secure environment, and will destroy all printed confidential information when my legitimate need for that information ends in a way that protects the confidentiality of the information.
8. I will follow Department of Speech and Hearing Sciences policies and procedures regarding the use of any portable devices that may contain confidential information including the use of encryption or other equivalent method of protection.
9. I acknowledge my obligation to report to the appropriate personnel any practice by another person that violates these obligations or puts the Department of Speech and Hearing Sciences, its personnel, or its patients at risk of disclosure of confidential information.

WASHINGTON STATE UNIVERSITY
Elson S. Floyd
College of Medicine

10. If I am involved in research, any research utilizing individually identifiable protected health information will be performed in accordance with federal, state, local and Institutional Review Board policies.
11. If I no longer need confidential information, I will dispose in a way that assures others cannot use or disclose it including the Information Technology policy for disposal of printed confidential information or electronic equipment that may contain confidential information.
12. I understand that my communication using the WSU information network is not private and the content of my communication may be monitored to protect the confidentiality and security of the data.
13. I understand that my obligation under this Agreement will continue after termination of my relationship with the Department of Speech and Hearing Sciences at Washington State University.
14. I understand that I have no right or ownership interest in any confidential information referred to in this Agreement. The Department of Speech and Hearing Sciences may at any time revoke my password, or access to confidential information. At all times during my relationship, I will act in the best interests of WSU' Department of Speech and Hearing Sciences.

Name (print) Date

Name (sign)