WASHINGTON STATE UNIVERSITY
Elson S. Floyd
College of Medicine

Confidentiality Agreement

Speech Language Pathology Services

As an employee or student in the WSU Department of Speech and Hearing Sciences ("DSHS"), you may have access to "Confidential Information." The purpose of this Confidentiality Agreement is to help you understand your duty to safeguard Confidential Information.

Definitions: "Confidential Information" includes Protected Health Information (PHI) and personally identifying information (PII) that you create, access, and/or receive as part of a clinical experiential learning activity, assignment, and/or function. PHI includes 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; and that identifies the individual, or concerning which there is a reasonable basis to believe the information can be used to identify the individual. *See* 45 CFR § 160.103.

As an individual having access to Confidential Information, you are required to conduct yourself in strict conformance with applicable laws, DSHS privacy and security policies, and clinical training sites privacy and security policies where you are assigned or performing DSHS activities. A violation of any of these duties may subject you to discipline, which might include, but is not limited to, dismissal or termination.

As a condition of your relationship to the DSHS, you are required to acknowledge and abide by these duties.

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 (i.e., PHI) at clinical training sites 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, face photographs and comparable images, other identifying numbers or codes.
- Deidentified PHI: Deidentification of PHI requires removal of all of PHI data elements and the remaining data alone or in combination with other information cannot be used to identify the individual.
- Research data including PHI created, collected, or used for research purposes.
- Third party information – including PHI contained within computer programs, client, and vendor proprietary information, or any other proprietary technology.
- PII used in other contexts. Defined above and is included as Confidential Information.

Examples of inappropriate disclosures of Confidential Information include:

- Accessing, discussing, or disclosing Confidential Information to friends, family, or posting it on social media.
- Using Confidential Information for a personal benefit, financial gain, and/or purposes including social. The unauthorized disclosure or use of Confidential Information by employees or students may subject each individual and the clinical training site to legal 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 dismissal or termination in accordance with WSU policies or guidelines.

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 to perform legitimate duties as defined by my relationship (faculty, employment, student, visitor, consulting, etc.) with the DSHS.

    - 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 DSHS and in accordance with the law and applicable policies.
    - I will not misuse or carelessly handle Confidential Information including posting Confidential Information on social media.
    - I understand that it is my responsibility to assure that Confidential Information in my possession is maintained in a physically secure environment.
    - I will become familiar with the clinical training sites privacy and security policies where I am assigned or performing duties and follow them and if I have questions seek clarification.

WASHINGTON STATE UNIVERSITY
Elson S. Floyd
College of Medicine

- I will deidentify all patient information in accordance with the HIPAA deidentification rule where I am authorized to use and need clinical information for academic purposes related to my placement, assignment, or duties.
  See *https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html*.

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 acknowledge 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 to safeguard my password or other authorization to access Confidential Information.
3. I will log off computer systems after use or when leaving my workstation.
4. I will not log on to an information 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 inappropriately misused or disclosed.
6. I will not download or transfer computer files containing Confidential Information to any non-authorized computer, data storage device, portable device, telephone, or other device capable of storing digitized data.
7. I acknowledge that Confidential Information created, accessed, or disclosed at a clinical training site should stay within that clinical training site including their information systems, and **should not** be shared, disclosed, and/or downloaded on WSU information systems (e.g., WSU email) or devices.
8. 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 properly dispose (e.g., locked shredder bins at the clinical training site) or destroy all printed Confidential Information when my legitimate need for that information ends.
9. I will follow security policies and procedures regarding the use of any portable devices that may contain Confidential Information including the use of encryption.
10. I acknowledge my obligation to promptly report any privacy and/or security concerns or violations in accordance with appropriate policies of WSU and/or the clinical training site. Individuals should contact the WSU COM Office of Compliance where questions arise.
11. If I am involved in research, any research utilizing PHI will be performed in accordance with federal, state, local and Institutional Review Board policies.
12. I understand that my obligation under this Confidentiality Agreement will continue after termination of my relationship with the DSHS and my clinical training program or activities.
13. I understand that I have no personal rights or ownership interest in any Confidential Information referred to in this Confidentiality Agreement. I acknowledge that earning the trust and confidence of patients/clients requires appropriate privacy/security safeguards be applied to prevent disclosure of Confidential Information. At all times during my relationship with DSHS, I agree to act in accordance with all applicable privacy and security laws, policies, and professional standards and ethics, and this Confidentiality Agreement.

Name (print) Date

Name (sign) Date