University of Puget Sound

Onsite Physical Therapy and Occupational Therapy Clinics

CLINIC OPERATIONS MANUAL AY 25-26

Revised 12-2023; 01-2025; 08-2025

The policies and procedures in this manual describe basic clinic operations common to both the Occupational Therapy and Physical Therapy Onsite Clinics. It is the responsibility of everyone in the clinic (students, faculty, clinical instructors and administrative staff) to be familiar with, and to adhere to these policies. Policies and procedures unique to each clinic (OT and PT) will be described in a separate document. Occupational therapy adult and pediatric participants volunteer in teaching clinics, and their information is not considered part of a medical record. The term patient is used throughout this manual with the understanding that occupational therapy clinic participants are not being seen as medical patients.

COVID-19 Policies and Procedures

Refer to Counseling, Health, and Wellness Services guidelines for the most up to date policies and procedures and Tacoma-Pierce County Health Department for updated masking and PPE guidelines for healthcare settings during respiratory illness season.

Reminder Calls

- Students will contact all patients by phone 1-2 days prior to their first visit. The phone call will include the reminder to not come to clinic if they are not feeling well.

Infection Control/Sanitization Procedures

Students are responsible for disinfecting their own clinic equipment, i.e., blood pressure cuffs, stethoscopes, gait belts, goniometers, etc. between each patient. Expendable supplies such as electrodes or Thera-band will not be shared between patients. Each patient will be issued their own supplies. Some supplies may be stored in plastic bags marked with the patient's name and retained in the clinic.

Emergency Procedures

Students and clinical instructors should familiarize themselves with all of the clinic spaces. All parties involved in the onsite clinics should be aware of the following locations and sounds:

- **Location of all exits from the clinic areas**
- **Location of all accessible exits**
- **Location fire alarms**
- **Location of fixed telephones**
- **Location of fire extinguishers on first and second floor**
- **Location of AED on first and second floor**
- **Location of bathrooms**
- **Sound of bathroom alarms**

Fire

1. Pull fire alarm!
2. Call 911 from a **landline** in the clinic **AND** call Safety and Security at **3311**. [NOTE: It is NOT necessary to dial "9" before calling 911 from a landline. Simply dial 911.] **Do not use personal cell phones**.
3. Report the building (**Weyerhaeuser Hall**) and **room number**
    1. Adult clinic **116** (ortho) **117** (neuro)
    2. Apartment **119**

3. Therapeutic Customization Lab **115**
4. Assistive Technology Lab and Driving Simulator **108**
5. Work Hardening Area **123**
6. Pediatric clinic **219**
7. Onsite Clinic workroom **105**
8. Resource Room **107**

4. Remove patients/clients from the building.
5. For small contained fires- use fire extinguisher – only after patients are safely out of the room.
6. Close all doors and windows.
7. All building occupants, including patients, should gather at the end of Commencement Walk on N.11th St. NOTE: Patients/clients who are not able to get to the designated gathering area at the end of Commencement Walk may gather on N. 11th St. outside the mobility park gate. Make sure that patients/clients are not in the driveway to the parking lot for Weyerhaeuser Hall.
8. Each student therapist is responsible for getting his or her patients/clients out of the building and to the designated gathering area.

Medical Emergency

1. Designate someone to call 911 **AND** Safety and Security at **3311** from a **landline** in the clinic. [NOTE: It is NOT necessary to dial "9" before calling 911 from a landline. Simply dial 911.] **Do not use personal cell phones.**
2. Stay with the person who is having the medical emergency, monitor health status, and provide measures of comfort until help arrives.
3. If the person becomes unresponsive, follow CPR/AED procedures.
4. Remove other patients/clients from the immediate area.
5. Station someone at the door to help emergency personnel locate the affected individual.

In case of Accident

1. Call 911 **AND** Safety and Security at **3311** from a **landline** in the clinic. [NOTE: It is NOT necessary to dial "9" before calling 911 from a landline. Simply dial 911.] **Do not use personal cell phones.**
2. Stay with the injured party and stabilize as necessary.

- If a patient/client is injured or has a medical emergency during a clinic session, stay with the patient and **immediately** send someone to notify a clinical instructor.
- If an injury occurs that does **not** require an emergency response, contact the patient/client's physician (and parent if appropriate) and follow the physician's recommendations.

After the medical emergency or crisis is resolved, the student and clinical instructor must complete an **Incident Report** form. The incident report must be completed on the day of the incident. A copy of the report must be hand delivered to the Director of Clinical Education for PT or the OT Faculty Clinic Coordinator. Following review by the DCE or OT Faculty Clinic Coordinator, a copy of the report should be placed into the person's medical record and a copy should be sent to the appropriate program director and to the University Vice President for Business Services. The Incident Report forms are available on the PT Clinic Network Share Drive and in the Resource/chart room 107.

Campus Emergency

The onsite clinic is a unique classroom environment. In the event of a campus emergency, students are responsible for their patient/client as well as themselves when following the appropriate response guidelines that are outlined on the first day of each semester and published in the course syllabus attached to the specific clinical course.

Mandatory Reporting Policies and Procedures

All licensed health care providers are mandated reporters and are required by law to make a report if they suspect the abuse, abandonment, neglect or exploitation of a vulnerable adult or if they have reasonable concern that a child is being abused, neglected or is unsafe at home. If you have concerns about any client/patient you are caring for in the onsite clinic, please do all of the following:

1. Express your concerns to your clinical instructor.
2. The licensed clinical instructor (CI) will determine the need for and proceed with filing the report.
3. For vulnerable adults, a report may be made to **Adult Protective Services** (APS) online https://fortress.wa.gov/dshs/altsaapps/OCR/publicOCR.PubRptInputReporterInformation.executeLoad.action or by calling (877) 734-6277.
   Reports may be made to **Child Protective Services** (CPS) by calling 1-866-ENDHARM (866) 363-4276.
   In some cases, the local police may need to be contacted as well. If local police are notified, Safety and Security must be contacted as well by calling (253) 879-3311.
4. Complete a Record of Mandated Reporting Incidence (available on the PT Onsite Clinic Network Share or School of Occupational Therapy Canvas page). Follow the directions for completing and submitting the form.

Standard Precautions for Infection Control

Hand Washing: Anyone who comes in physical contact with clients/patients must either wash their hands or use hand sanitizer **before and after** each encounter.

Gloves and Masks: Gloves must be worn when performing treatment interventions that may put the clinician in contact with body fluids such as oral-motor or toileting activities. In addition, gloves must be worn any time a clinician comes in contact with bodily fluids.
Masks must be worn to protect mucous membranes if the therapy intervention involves possible release of body fluids into the air such as during wound care.

Routine Equipment Cleaning: The entire clinical staff is responsible for maintaining a clean clinic environment. Equipment, including mats, treatment tables, therapy balls, etc. must be cleaned with disinfectant between **each** client/patient use. All equipment must be cleaned with disinfectant spray and at the end of each therapy day. The student therapist who has used the equipment is responsible for cleaning it.
Students are responsible for disinfecting their own clinic equipment, i.e., blood pressure cuffs, stethoscopes, gait belts, goniometers, etc. between each patient. Expendable supplies such as electrodes or Thera-band will not be shared between patients. Each patient will be issued their own supplies. The supplies will be stored in plastic bags marked with the patient's name and retained in the clinic.

Sanitizing Toys: Make a sanitizing solution of ¼ cup of household bleach to one gallon of water. Diluted bleach is considered safe for cleaning children's toys since chlorine evaporates quickly. Fill sanitizing tub or bucket to line with water and add ¼ cup of bleach. [Bleach is kept in the upper locked cabinet in the pediatric clinic WEY 219 that is marked "Cleaning Supplies". A key to this cupboard is hanging on a hook inside the cupboard next to it.]
Dip toys in the bleach solution and place in the drying rack to air dry. If the toy cannot be immersed in water, spray the same solution on the toy and wipe it thoroughly. Once the toys have air dried, they should be returned to the correct place.

NOTE: Bleach is only to be used in the pediatric clinic for cleaning of toys or other small items that children may place in their mouths and should not be used for any other cleaning/disinfecting tasks. Bleach MUST be stored in a locked cabinet at all times.

Linen

The university contracts with Superior Linen for linen rental and cleaning. All linen belongs to Superior Linen. PT laundry bins and laundry bags used for dirty laundry are **GREEN**; PT towels and sheets are **Off-White**. OT laundry bins and dirty laundry bags are **RED**. OT towels and sheets are **WHITE**.
Superior linen is stored in Weyerhaeuser 106 with additional stock stored in WEY 116 and 117, respectively. Soiled linen is to be placed in the GREEN (PT) or RED (OT) barrier bags respectively and the full bags are to be placed in the storage bin in WEY 106. NOTE: OT (GREY) and PT (WHITE) have a small stock of linen and should not be disposed of in the green OR red barrier bags provided.

Biohazardous Waste Disposal

Trash contaminated with blood or drainage:
Contaminated dressing materials, etc. should be disposed of in a red bag in the Biohazard Waste container located in the private exam room WEY 125. The bag in which the materials are placed should be secured and Facilities Services should be contacted at extension 3231. **When Facilities Services is notified, please let them know the contents of the bag.**

Trash contaminated with body fluids other than blood (urine, vomit, feces):
Contaminated trash such as soiled diapers, wipes, catheters, etc. should be DOUBLE BAGGED and disposed of in a regular trash can. The bag in which the trash is placed should be securely closed and Facilities Services should be notified to dispose of it. **When Facilities Services is notified, please let them know the contents of the bag.**

NOTE: Parents may be asked to take soiled diapers and dispose of them after leaving the building. Plastic bags are provided in WEY 219 if needed.

Linen contaminated with body fluids:
Linen soiled with small amounts of body fluids must be placed into a plastic trash bag which is tied off. The plastic bag should then be placed into the soiled linen bin or bag. If linen is saturated with urine or soiled with stool, it should be placed into a plastic bag, securely closed and placed in a trash can. Facilities Services should be notified to dispose of it. If linen is saturated with blood, it must be labeled CONTAMINATED. **When Facilities Services is notified, please let them know the contents of the bag.** The department/clinic receptionist should be informed as to the type and number of sheets, towels, etc. that have been disposed of so that the linen can be properly accounted for by the linen service provider.

Chemical Exposure

Material Safety Data Sheets are maintained in the administrative office (WEY 105) for all substances used in the Physical Therapy and Occupational Therapy programs that may be hazardous. For the clinic this includes the cleaning materials. If a spill occurs, follow the MSDS information for personal exposure and contact Facilities for clean-up.

Dressing and Grooming

a. By Washington State law, name tags must be worn at all times by student therapists and clinical instructors. All students must wear a photo ID name badge.
b. Appropriate clothing is to be worn for clinic. Jeans, leggings, yoga pants or shorts are not allowed. Cropped pants (above the ankle) are acceptable provided that they are not made of spandex or materials typically used for work-out clothes. No clothing with clinic names/logos (except for UPS), no bare midriff attire, no exposed chest, no exposed buttocks, no visual undergarments etc. Clothing should also accommodate movement and not be tight fitting. Students should be able to vigorously move without exposing any portion of the skin on the midriff, buttocks or chest or any undergarments. Lab coats will be required if your CI determines your attire to be inappropriate.
c. Shoes: no open-toed or open-backed shoes, no heels. Clean sports shoes are permitted. All laces must be tied.
d. Facial piercings, e.g., earring, eyebrow, nose & lip rings, nose studs, etc. should be worn with caution, as they may be accidentally caught or pulled out.
e. No excessive cologne, after shave; perfume, essential oils, etc.
f. Fingernails should be trimmed and clean.
g. Hair should be neat and be tied back if long.
h. Hands are to be washed with soap and water or disinfected following each patient/client contact.

Smoking

The Onsite Physical Therapy and Occupational Therapy Clinics and all surrounding areas of Weyerhaeuser Hall are NON-SMOKING. Students should investigate and immediately report any evidence of smoking.

Food and Drink

Food and drinks **are not allowed** in **ANY** of the following clinical spaces at any time: 105, 115, 116, 117 , 123, 216 or 219. Food and drinks are allowed in the kitchen area (119) and the pediatric clinic (219) only if they are part of a therapeutic intervention.

WEY 105 Workroom Use Policy

The student work room in WEY 105 has been set up to support the work occupational therapy and physical therapy students need to do for clinic. Priority for use of the work room is given to students who have clinic that same day. We realize there may be clinic activities such as phone calls or preparation for an upcoming clinic day that may need to occur on one of your non-clinic days. However, please be sensitive to those students who are currently in clinic and may need to access the phone or computer quickly between clients.

The printer, fax, computer, telephone etc. in WEY 105 are for **clinic purposes only**. This means printing single copies of client medication lists, score forms for standardized tests, etc. and faxes related to clinic needs only. **The fax machine is <u>not</u> a printer and should not be used as such.** The clinic receptionist can assist with copy needs. The computer is set-up as a standing station to facilitate quick periods of use only. This station is not intended for clinic documentation or completion of class assignments. Please use dedicated computer labs either in WEY or elsewhere on campus for longer projects. Space is available in WEY 107 and 115 for these activities.

Problems with equipment in WEY 105 should be reported to the administrative assistant that supports the respective clinic. If neither of them is available, notify your Clinical Instructor and call Technology Services. **DO NOT** disconnect cables, etc. or attempt to make repairs yourself. **DO NOT** walk away and leave the problem for someone else to address.

<u>Computers in CI Offices</u>

The computers in the CI office (WEY 126) are not for student use. Students MAY use the computers in the pediatric CI office (WEY 219) however its use is limited to clinic needs only. Students who need computers for other purposes should use one of the designated computer labs on campus.

<u>Storage of Personal Items</u>

Personal belongings *other than* personal clinic equipment such as gait belts, blood pressure cuffs, stethoscopes, goniometers, etc. are not allowed in the clinic space when the clinic is in operation. Personal effects, including backpacks, laptop computers, coats, etc., should be stowed in room 106 for adult clinic and in the pediatric clinic Clinical Instructor office for pediatric clinic. Although both of these locations are secure from the general public, all students do have access. The OT and PT programs and the university are not responsible for losses of items stored in these areas.

<u>Technology Lab WEY 108 and Technology Equipment Policy and Procedures</u>

***NOTE: Lab manager hours are posted on the door of 108**

The computers in this lab are set-up with specialized software and hardware and should not be used for general computing. Due to the specialized software and hardware on the computers, students may encounter difficulties including crashed profiles if the computers are used for general computing. These computers cannot be encrypted and therefore cannot be used for clinic documentation.

Due to the cost of some of the equipment, it is locked up unless the lab manager is in the lab or unless a student has made a reservation to use the equipment and arranged for a cabinet to be unlocked ahead of time.

<u>Reservation of Equipment</u>

It is strongly recommended that you reserve equipment at least 2 days prior to when you want to use it. Reservation forms are outside of the door of WEY 108 in the hanging file folder. Some general guidance regarding reservations

1. You can only reserve 2 weeks at a time (this allows everyone equal access to the equipment).

2. You must be checked out by the lab manager or staff prior to reserving the Wii, Kinect or iPads so you know how to set-up, recharge and/or use the equipment correctly.
3. During times when clinic is in session, priority reservation first goes for clinic use, second for class use and third for practice. Reservation for practicing or learning any equipment, software or hardware should be done during non-clinic hours or when the equipment is not needed for a class.

Checking out and in the Equipment

Equipment that is removed from WEY 108 must be checked out and in via the lab manager, your clinical instructor/faculty member, the OT administrative assistant (or a resource room worker). The Equipment Reservation Forms will be reviewed by these individuals so they are prepared to help you; if you do not make a prior reservation for your equipment, you may not be able to check it out at the last minute if someone is not available to check it out. When checking out equipment

1. Check-out is for one hour time blocks; unless otherwise specified or special arrangements have been made.
2. Make sure you list everything you take on the correct equipment check-out form in WEY 108.
3. Some equipment (including Wii, iPads, etc…) can be checked out overnight when prior arrangement has been made with the Assistive Technology Lab Manager.

When checking in equipment

4. Your equipment will be checked to make sure it is returned in working order. We understand that accidents happen. If a piece of equipment is broken, please let the lab manager know right away so it can be repaired or replaced.
5. Make sure everything is connected to the correct charger.
6. Make sure you return everything to the correct storage space.
7. Make sure you have put all software/Wii games, etc… into the correct containers.

Requesting New Software, Hardware, Technology Equipment and/or Apps

Forms are available in WEY 108 for requesting additional software, hardware, technology equipment and/or apps currently unavailable in the lab. Please plan ahead as approval and procurement and/or the downloading of some of these items could take several days. The appropriate form must be completed before anything will be considered or ordered. Copies of the form can be found in WEY 108 or on the Clinic Canvas page.

Printing-OT

There is a small black and white printer available in WEY 108 for printing data specific to the Dynavision and the Driving Simulator ONLY. If color printing is required for clinic purposes, please complete a Clinic Supplies Request Form (link on Canvas) and email (or tag) the OT Clinic Assistant at otclinic@pugetsound.edu. All requests may not be approved, so please be sure that color printing is essential.

Photos and Videos

Photography consent forms must be completed for **all** still or moving images according to the procedures described in the HIPAA Privacy Policies in this document.

Patient/client pictures and videos are **ONLY** to be taken with iPad Mini #1 (black OtterBox)

- Media will be transferred from iPad to encrypted computer in AT lab 2x/wk.
- To protect client confidentiality, media will be deleted from the computer after **one week**.
- Make an appointment with the AT lab manager during scheduled AT lab hours to retrieve media.
- Videos and pictures can be uploaded to an encrypted thumb drive for later use. Contact the respective clinic admin (OT or PT) for a thumb drive.
- To schedule a meeting outside of office hours, please contact the AT lab manager.

Resource Room Materials Check-out Policies

- All assessments and other items must be checked out with Resource Room staff.
- Check out items for yourself only; not for your classmates.
- There is a 2 hour check-out limit for all items.
- Overnight check-out is acceptable only during the last 2 hours of the RR operating hours for that day. Items that are checked out overnight must be returned by 8:00AM Fall Semester, 7:00AM Spring Semester the following day.
- Items checked out the last 2 operating hours on Saturday may be kept until Monday at 8:00AM Fall Semester, 7:00AM Spring Semester.
- Items checked out during clinic are allowed to be out for the entire clinic time.
- Check-out time may be extended if an email request is sent to *otptresourceroom@pugetsound.edu* by the course faculty member or clinical instructor.
- Original assessments and scoring sheets for standardized tests are for use with clients ONLY. Copies may be requested for practice use.
- If returning an item after RR hours, please complete a return slip and place the item(s) in the return bin just inside the RR door.
- Failure to adhere to these policies will affect your professional behaviors in the onsite clinic and may result in a *Notice of Clinical Deficiency*.

Respecting Patient/Client Privacy, Dignity and Preference

The UPS Onsite Clinics follow the **University of Puget Sound HIPAA Privacy Policies and Procedures** regarding the handling and safeguarding of protected health information (PHI). See Appendix A.

The fundamental mission of the Onsite Clinics is the clinical education of the student therapists. Patients/clients should be reminded of this mission during the first visit. Patients/clients should be specifically informed that information about their case will be discussed amongst the treating therapy group and with the clinical instructors. All patients/clients should be informed that it may be beneficial to student learning for them to participate in demonstrations. Patients/clients must be informed that they have a right to decline to participate in any activity for the sole purpose of clinical education.

Photographic or video images require completion of a specific patient/client consent form. The consent form allows the individual to consent to use of the images for treatment and documentation only and separately allows the individual to give consent for the images to be used for educational purposes. No

patient/client images will be used for anything other than treatment or educational purposes unless specifically stated on the consent form. No photographic or video images may be taken on a student's personal electronic devices. All images placed on university-owned devices must be transferred onto an encrypted thumb drive that must be returned to the clinic at the end of each clinic semester. A Photography Consent form must be completed and maintained in the medical record for all images that become part of the medical record. Photographs and/or videos MAY be taken on a patient's personal electronic device as long as no copies are retained in the medical record. No other patients or students should be in any images without their written permission.

Medical Records Retention: PT ONLY

All Medical Records for Physical Therapy patients participating in the Onsite Clinic have been maintained in WebPT, an EMR (Electronic Medical Record) in use since 2017.

Washington State requires medical records to be retained for a period of seven (7) years. For minors, the records are retained until the minor child reaches the age of 26. UPS will treat all records the same and at seven (7) years post discharge from therapy or seven (7) years after the delivered service the medical records will be destroyed (burned or shredded).

OT/PT Consultation Process

Fall Semester

PT to OT Consult

1. PT student discusses the need for an OT consult with his or her clinical instructor.
2. If the clinical instructor agrees, the PT student completes an OT/PT Consultation Request form.

NOTE: Consultation requests for splints or custom adaptive equipment should be submitted no later than four weeks before the end of clinic. The OT Faculty reserve the right to defer any consultation made in the last four weeks of clinic if she or he determines that the time frame is not reasonable for completing the consult. For fall clinic patients, keep in mind that the consultation process will take longer for patients on a once-a-week schedule, unless they can attend clinic for additional OT sessions.

3. The completed form is forwarded to the adult OT clinic coordinator for review and processing.
4. The consultation is scheduled within one week of receipt of the request.
5. OT consults that take place during a patient's PT clinic appointment time should be limited to one OT faculty member and one OT student.

NOTE: It is unlikely for a PT consult to be initiated by someone in OT during the fall term. If the need for a PT consult should arise, the completed OT/PT Consultation Request form should be forwarded to the PT Onsite Clinic Coordinator.

Spring Semester

PT to OT Consult for Patient/Client who is NOT also being seen in OT clinic

1. PT student discusses the need for an OT consult with their clinical instructor.
2. If the clinical instructor agrees, the PT student completes and OT/PT Consultation request form.
3. The completed form is forwarded to the OT adult clinic coordinator for review and processing.
4. The consultation request is scheduled within one week of receipt of the request.

PT to OT Consult for Patient/Client who IS also being seen in spring OT clinic

1. PT student discusses the need for an OT consult with their clinical instructor.
2. If the clinical instructor agrees, the PT student and CI complete an OT/PT Consultation request form and have a discussion with the OT student and CI responsible for working with that patient.
3. The consultation request is scheduled within one week of receipt of the request.

OT to PT Consult for Patient/Client who is NOT also being seen in PT clinic

1. OT student discusses the need for a PT consult with their clinical instructor.
2. If the clinical instructor agrees, the OT student completes an OT/PT Consultation request form.
3. The completed form is forwarded to the PT Clinic Onsite Clinic Coordinator for review and processing.
4. The consultation request is scheduled within one week of receipt of the request.

OT to PT Consult for Patient/Client who IS also being seen in spring PT clinic

1. OT student discusses the need for a PT consult with their clinical instructor.
2. If the clinical instructor agrees, the OT student and CI complete an OT/PT Consultation request form and have a discussion with the PT student and CI responsible for working with that patient.
3. The consultation request is scheduled within one week of receipt of the request.

Policy Regarding Gifts

Patients will sometimes want to give gifts to student therapists or clinical instructors as a thank you. The Onsite Clinic abides by the APTA's Code of Ethics and Guide for Professional Conduct and the AOTA 2020 Occupational Therapy Code of Ethics with respect to gifts. Specifically, cash in any amount cannot be accepted. The student should thank the patient and explain that they cannot accept cash individually by a student. However, a student may let the patient know that a monetary gift can be donated to the clinic. The student should send the patient a thank you note and indicate that the funds were donated to the respective clinic.

Gift cards worth more than $5.00 should be returned to the patient along with a thank you note. The student should express appreciation but explain that clinic policy is that they are not allowed to keep gifts. Gift cards worth $5.00 or less are okay. Consumables such as cookies or candy (or flowers) are acceptable if they can be shared by all students in the clinic.

APPENDIX A.

HIPAA
Privacy Policy & Procedures

Revised 07/2020

INTRODUCTION

HIPAA is the "**H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct." It is Public Law 104-191, enacted August 21, 1996. The law was initially developed to enable individuals to carry health insurance during the time between their separations from one job to another job with a different employer ("portability").

Related provisions were later added to simplify the business of health care delivery and payment, and to guard against fraud and abuse in the health care industry ("accountability"). This part of the law is known generally as "Administrative Simplification." It refers to the business aspect of health care and the individual's right to information privacy.

Administration Simplification has two main purposes:

1. Standardize the way financial transactions are transmitted between providers of health care and paying organizations.
2. Establish standards for the privacy and security of **Protected Health Information (PHI).** Protected Health Information is personally identifiable health information in any form that is used, disclosed or managed by any entity covered by HIPAA.

Administration Simplification has three parts:

- The privacy aspect of HIPAA includes information privacy (patient/employee) and confidentiality (staff/employer). **Information privacy** is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.
  Confidentiality is the duty of individuals who have possession of information about others, especially in the course of particular kinds of relationships with them, not to use or release information inappropriately.

- The security aspect of HIPAA describes the physical, administrative, and electronic actions taken to safeguard information against improper use, disclosure, or change. Security measures like passwords, locks, and privacy screens enable a healthcare provider to protect a patient's privacy. However, it is the individual's responsibility to handle and use the information appropriately that is the key to making this provision successful.

- The transactions, code sets and identifiers make up the third part of Administrative Simplification called EDI or Electronic Data Interchange. This aspect of the law was developed to achieve good business practice for claims transactions. It standardizes the format for EDI and creates single identification numbers for industry participants.

The University of Puget Schools of Occupational Therapy and Physical Therapy, hereafter called "Facility", **has adopted the following policies and procedures to comply with the HIPAA standards, the Department of Health and Human Services (HHS) regulations, and state laws regulating privacy, security and transactions/code sets. These policies and procedures apply to the onsite clinics and any community-based teaching clinic experiences required in either the Occupational Therapy or Physical Therapy program.**

PRIVACY POLICIES AND PROCEDURES

Training

All personnel who have access to PHI must complete HIPAA training and sign a confidentiality agreement annually. This includes students, office staff, core faculty and clinical faculty (clinical instructors). Students must also complete a student PHI contract that further explains confidentiality policies and procedures used in the onsite clinics and community-based teaching clinics. A record of training and signed confidentiality agreement must be retained by the respective clinic coordinator. See Appendices A-C.

Section 1 Use and Disclosure of Protected Health Information

The policy of the *Facility* is to protect the privacy of individual patient health information. The Facility will make reasonable efforts to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose.

Protected Health Information (PHI) in the *Facility* is defined as any individually identifiable information, whether paper, electronic (emails, data bases and backup tapes), verbal (in person, by phone, voice mail, and dictation), electronic media including still photographs, videos or DVD, or faxes. The Privacy regulation protects clinical and treatment information, payment information, and information that either directly identifies the patient or creates a reasonable basis to believe that the information can be used to identify the patient. The following list includes examples of PHI:

- Medical records
- Treatment plans
- Prescriptions/Authorizations/Referrals
- Claims/Billing Codes/Billing Statements
- Appointments
- Evaluations/Progress Notes/SOAP Notes/Discharge Summary
- Medical history/Family history/Medication information
- Demographic data
- Informed consent documentation
- Voice mails and emails with patient specific information
- Conversations regarding a patient's health status, treatment and bills
- Back-up copies of all of the above

The *Facility* may use and disclose protected health information without patient authorization for treatment, payment, and health care operations. Some examples of disclosure of PHI are:

- Upon request of the patient
- If needed for health care treatment, payment, or operations (includes, but not limited to, coordination of benefits, quality improvement, risk management, training, prescriptions, peer review, utilization review, obtaining professional liability insurance, and scheduling appointments)
- If request is from a health care provider to a laboratory or pharmacy
- To provide care to an inmate of a correctional facility
- If the request is made by a representative of an accrediting body
- To detect health care fraud or abuse
- To detect health care compliance.

Requests for PHI are limited to individuals who need the information to carry out patient care duties. These individuals are:

- *Physical therapists/Occupational Therapists*
- *Physical therapist assistants*
- *Ancillary personnel, i.e. physical therapy aides, front office personnel*
- *Physicians*
- *Physician assistants*
- *Nurse practitioners*

- *Consultants*
- *Physical therapy and occupational therapy students involved in patient related activities*

Other individuals who may receive Protected Health Information are:
- Other providers
- Family members
- Law enforcement officials
- Emergency personnel
- Auditors
- Health plan reviewers
- Billing services
- Employers
- Insurance companies
- State agencies
- Attorneys (judicial and administrative proceedings)
- Accountants

The amount of PHI provided for each request is limited to:
- *Complete legal name, address, and telephone number*
- *Date of birth*
- *Social security number*
- *Past medical history information*
- *Documentation of completed evaluations, progress notes, tests, SOAP notes, etc.]*
- *Attendance records*
- *Signed release forms*
- *CPT code form*

Each written request for PHI by individuals or entities not directly involved in providing patient care are to be maintained by the clinic and retained for a period of seven (7) years.

PHI is maintained in the locations listed below in this clinic:
- *File cabinets/rooms*
- *Computer databases*
- *Archives*

PHI is disposed of in the following ways at this clinic*:*
- *Shredding*
- *Deleting computer files*

Electronic Communication

The HIPAA Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. See 45 C.F.R. § 164.530(c). Although the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail.

Note that an individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable. See 45 C.F.R. § 164.522(b). For example, a health care provider should accommodate an individual's request to receive appointment reminders via e-mail, rather than on a postcard, if e-mail is a reasonable, alternative means for that provider to communicate with the patient. By the same token, however, if the use of unencrypted e-mail is unacceptable to a patient who requests

confidential communications, other means of communicating with the patient, such as by more secure electronic methods, or by mail or telephone, should be offered and accommodated.

Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that limited e-mail communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications. Patients may request that email be used for communication purposes, however information exchanged in that manner must be kept to a minimum.

In order to ensure compliance, email communications between provider and patients are limited to appointment reminders and general treatment instructions such as home exercise programs or directions for applying an orthotic, etc. Email communications may not include actual treatment notes.

Medical Record Retention

Washington State requires patient files to be retained for a period of seven (7) years. For minors, the records are retained for three years after the patient becomes of legal age under State Laws or seven (7) years after the date of discharge. Records will be burned or shredded after the required retention time has expired. A log containing the names of the individuals whose records have been destroyed must be maintained in the relevant administrative office (OT or PT) in perpetuity.

Section 2 Authorization

A signed Authorization form from an individual is not necessary before using or disclosing protected health information (PHI) for treatment, payment, or healthcare operations. A signed Authorization form is required if PHI is to be used or disclosed for any of the following:

1. internal or external outcomes marketed to other providers,
2. research that has not been reviewed by a privacy board or institutional review board,
3. marketing of health and non-health items and services,
4. sale, rental, or barter,
5. eligibility for employment determinations,
6. fundraising,
7. students in a "job shadow" program,
8. application for life or disability insurance,
9. banking services,
10. eligibility for enrollment in a health plan.

The Authorization form is signed and dated by the individual and retained in the medical record for seven (7) years.

The Authorization form must include the following:

1. a specific description of the information to be used or disclosed,
2. identification of the covered entity authorized to use or disclose the PHI by the authorization,
3. identification of a specific person or persons that would be allowed to use or receive the PHI,
4. a specific expiration date,
5. a signature or other authentication (e.g., electronic signature) and the date of the signature,
6. a statement that individual understands that he or she may revoke an authorization except to the extent that action has been taken in reliance on the authorization,
7. a description of how individual may revoke the authorization,
8. a statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by the federal regulations governing the Privacy of Individually Identifiable Health Information (45 CFR Part 164),
9. a description of a representative's authority to act for the individual in cases where the authorization is signed by a personal representative of the individual.

The following policies will be in effect if the Authorization form is initiated by the clinic in order to send information to a person outside of the organization for purposes other than treatment, payment, or health care operations.

1. Authorization form is completed.
2. Authorized use or disclosure of minimum necessary to accomplish the purpose specified in the authorization is adhered to.
3. All of the above mentioned elements are also present in the authorization when another covered entity requests that you obtain authorization for the use or disclosure of PHI to that covered entity to carry out treatment, payment, or healthcare operations.

Authorization is not required from the patient when requested under the following circumstances:

1. treatment,
2. payment,
3. health care operations,
4. release to the patient,
5. release to business associate,
6. as required by law,
7. judicial and administrative proceedings,
8. health oversight agencies,
9. law enforcement officials,
10. public health agencies, FDA, reporting communicable disease,
11. coroners, medical examiners, and funeral directors to carry out their duties as required by law
12. for specialized government functions, including military and veterans activities, national security and intelligence activities, protective service for the President and others, medical suitability determinations, correctional institutions and other law enforcement,
13. for victims of abuse, neglect, or domestic violence,
14. to avert a serious threat to health or safety,
15. workers' compensation or other similar programs, established by law.

AUTHORIZATION TO USE AND/OR DISCLOSE MEDICAL RECORDS

I hereby authorize _____ to use and/or disclose a copy of the specific
(Name of health care provider)
Health and medical information identified below for _____ to the following
(Name of patient/client)
Individual or entity _____.
(Name and address of recipient)

List of information to be used/released: _____

_____.

1. I understand that if the person or entity receiving this information is not a health care provider or health plan covered by federal privacy regulations, the information described above may be re-disclosed and no longer protected by those regulations. However, the recipient may be prohibited from disclosing substance abuse information under the Federal Substance Abuse Confidentiality Requirements.

2. *[If applicable]* I also understand that the person I am authorizing to use and/or disclose the information may receive compensation for doing so.

3. I further understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment, payment or my eligibility for benefits.

4. I may inspect or copy any information to be used and/or disclosed under this authorization.

5. Finally, I understand that I may revoke this authorization in writing at any time except to the extent that action has been taken in reliance upon this authorization. The revocation of authorization must be submitted to

   _____ at _____.

6. This authorization expires on _____.

_____ _____
Signature of patient/client or personal representative Date

_____
Print patient/client name

_____ _____
Print personal representative name Relationship to patient/client

_____ _____
Clinic representative/witness Date

Revised 12-2023; 01-2025; 08-2025

Section 3 Minimum Necessary Standard

The *Facility* takes reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose.

The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes
- Disclosures to the individual who is the subject of the information
- Uses or disclosures made pursuant to an individual's authorization
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes
- Uses or disclosures that are required by other law

The following categories of individuals are permitted unrestricted access to PHI for the purpose of providing patient care:

- *Physical therapist, occupational therapists, front office personnel, ancillary staff, billing personnel, physical therapy and occupational therapy students*
- *The categories or types of protected health information needed include the entire medical record.*
- *The conditions for access to PHI include Facility current employees and currently enrolled students.*

The clinic may provide limited protected health information upon request if the request is made by *another physical therapy clinic, hospital, physician, or other health care entity.*

Non-routine disclosure or requests will be reviewed on an individual basis and limited to only the minimum amount of protected health information necessary to accomplish the purpose of the disclosure or request.

Section 4 De-Identified Information

De-identified health information is information that has been stripped of all elements that could potentially identify the individual who is the subject of the protected information, i.e. individually identifiable information. Health information that is de-identified is not subject to the HIPAA regulations.

Identifiers will not be removed when it will affect the delivery of safe and effective health care to the individual. However, identifiers will be removed when possible from PHI used for:
research, training, and quality assurance activities.

The following list of identifiers will be removed when possible:

- Demographic information
- Name, street address, city, state, zip code
- Phone number, fax number, email address
- Precinct
- Dates: birth, death, start treatment, discharge
- Social security number
- Payment history
- Account number
- Name and address of provider and/or plan
- Numbers for: account, health plan beneficiary, medical record, certificate/license, vehicle or other devise serial number
- WEB Universal Resource Locators (URL)
- Internet Protocol (IP) address numbers
- Finger or voice prints

- Photographic images
- Any other unique identifying number or characteristic code
- Any other information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

Such de-identified information may be used in any way, provided that the key or other mechanism that would enable the information to be re-identified is not released to any other organization and that the Facility reasonably believes that such use or disclosure of de-identified information will not result in the use or disclosure of PHI. The clinic can use an identifier only if the identifier cannot be linked to an individual.

Photography

Photographic images, including still images, digitized images and videos of the patient are considered part of their health record. As such, they need to be handled in the same manner as other types of PHI. A photograph or video image that identifies him/her cannot be posted in public areas, such as hallways, without specific authorization from the patient. Similarly, a photograph that identifies a patient cannot be used in any form of publication without the patient's specific authorization. If the patient is not identifiable from the image, it is not considered to be PHI. A copy of the Consent for Photography can be found in Appendix D.

Specific HIPAA compliant authorization is NOT necessary if the photographs or videos do not contain actual patients and are used internally for training purposes or other activities that fall under the umbrella of health care operations. In this case, a general consent for photography is sufficient. If an image is made available to the public in any format, it is recommended that photographs of actors portraying patients be identified as simulations. Therefore, in order to ensure compliance and avoid confusion, images of actors portraying patients that will be available to the public in any format, e.g., photographs or videos that are posted on websites, informational brochures, etc. must be identified as simulations.

Patients/clients must be compensated at least $1.00 for publishing rights for any still images or videos are readily identifiable that will be used for promotional purposes in brochures, posters or on websites that can be viewed by the public. A receipt for payment must be attached to the photography consent for any images used for these purposes.

Section 5 Business Associates

A business associate relationship exists when a person or entity outside of the clinic (not a clinic employee or volunteer) performs a function or activity on behalf of the clinic that involves the use or disclosure of PHI; creates or obtains PHI on behalf of the clinic; or provides one of the services listed below to the clinic, involving the use or disclosure of PHI.

HIPAA provisions have been included in future contracts with business associates or have been added as addendums to current contracts with business associates. The Business Associate Contract can be found in Appendix E.

Business Associate Agreement Provisions

1.1 Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

1.2 Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions,

Notice of Privacy Practices

Facility's written Notice of Privacy Practices is given to patients on the first service date for review, signature (acknowledgement of receipt), and date. A copy is given to the patient and a copy is retained permanently in the onsite clinic office. If an acknowledgment cannot be obtained, the clinic staff will document the efforts to obtain the acknowledgement and the reason why it was not obtained.

This notice is to be given to the patient as requested any time after the first visit and is posted in a clear and prominent location in the waiting room. If our Notice of Privacy Practices changes, a copy of the revised notice will be available to the patient upon request. In addition, the revised copies will be available in the clinic and posted in the clinic.

The organization will retain a copy and any revisions of the Notice of Privacy Practices for seven (7) years.

On-Site Clinics

Statement of Privacy Policies

Revised 8/2017; Reviewed 7/2019, 12/2022, 12/2023

We understand that information about you and your health is personal. Thus, we are committed to protecting that information. This notice will tell you about the ways we use and disclose medical information about you while you are receiving therapy services at the On-site Clinics at the University of Puget Sound. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information.

Protecting your Personal Healthcare Information (PHI)

We use and disclose the information we collect from you only as allowed by the Health Insurance Portability and Accountability Act (HIPAA) of the State of Washington. This includes issues related to your treatment and transportation to and from the clinic, if needed. Your personal health information will never be otherwise given to anyone who is not involved in your care without your written consent. You, of course, may give written authorization for us to disclose your information to anyone you choose, for any purpose.

Our students, staff, and faculty are trained to make certain that the confidentiality of your records is always protected. Our privacy practices policies apply to all former, current, and future patients so you can be confident that your protected health information will never be improperly disclosed or released.

Collecting Protected Health Information

We will only request personal information needed to provide quality therapy services and to comply with the law. This may include your name, address, telephone numbers, medical history, health records etc. If we are collaborating with another health care provider on a billable service (e.g. provision of equipment) we may request social security or other insurance identification numbers. While most information will be obtained from you, we may also obtain some information from third parties if necessary (e.g. equipment). Regardless of the source, your personal information will always be protected to the full extent of the law and you will be informed prior to the release of your PHI.

Disclosure of your Protected Health Information

As stated above, we may disclose information as required by law. We are obligated to provide information to law enforcement and government officials under certain circumstances. We may call you regarding appointment reminders, but will be discretionary about the information stated on voicemail and answering machines.

Patient Rights

You have a right to request a copy of your health care information; to request a copy in a variety of formats; to request a list of instances in which we have disclosed your protected information for uses other than that stated above. All such requests should be stated in writing. We may charge for your copies in an amount allowed by law. If you believe your rights have been violated, please notify us immediately.

Patient's Rights

These provisions are intended to facilitate the individual's understanding of and involvement in the handling of their PHI.

Authorization Form & Right to Revoke Authorization
The authorization form will be used to obtain individual authorization before using or disclosing PHI to a non-covered entity.

Procedure:
1. Determine if an authorization is needed from a patient to release PHI.
2. Review the purpose of the authorization with the patient.
3. Ask the patient to read, complete, sign and date the authorization form on the designated areas.
4. Provide the patient with a copy of the signed authorization form.
5. Place the completed authorization form in the patient's medical record.
6. Explain that the authorization form can be revoked at any time. This revocation must be in writing and submitted to: *University of Puget Sound, Schools of Occupational Therapy and Physical Therapy, 1500 N. Warner #1030, Tacoma, WA, 98416-1070.* The clinic will retain the signed authorization form for seven (7) years in the patient's medical record.

(See "Authorization to Use and/or Disclose Medical Records" form.)

Patient Right to Receive PHI Upon Request
Patients are allowed to request access, inspection, and copying of their own PHI that is maintained in their medical chart or in the billing system.

Any requests for PHI by a patient are to be made in writing. The clinic does not require an explanation from the patient as to why the patient wants a copy of their PHI.

Determine if the patient has any grounds for the request to be denied, i.e. jeopardizing the safety of the patient or another person. If the request is not harmful to the patient or another person, the PHI will be provided to the patient within 15 days in hard copy form. The patient can either arrange a time to pick up the information or request that it be mailed.

The clinic documents the information requested on the PHI Disclosure Log in the patient's medical record and it is kept for seven (7) years.

Any information compiled for use in a court of law cannot be supplied to the patient.

The clinic may deny the request for PHI if the patient is an inmate of a correctional facility and if the information could harm the health, safety, security, custody or rehabilitation of the patient or other inmates, or the safety of any officer, employee or other person at the facility responsible for the transportation of the inmate.

If access to the information is denied, the clinic will provide the patient with a written explanation of why the access was denied. Information to file a complaint with the clinic is included with the denial (includes the name of the person to file the complaint, title, address and telephone number). The patient may request that the denial be reviewed. A licensed health care professional, other than the person who denied the request, will conduct the review. The clinic will comply with the outcome of the review.

Patient Right to Restrict Use of PHI
Patients are allowed to request that their health information not be used or disclosed for treatment, payment, or health care operations (except for those required by law). However, the clinic does not have to agree with the patient's request.

If the request is allowed, documentation of agreements of restriction and the termination of such agreements must be made in the patient's record and kept for seven (7) years.

Revised 12-2023; 01-2025; 08-2025

Accounting of Disclosures

Patients are allowed to request a list of instances when their PHI was released over the last seven (7) years prior to the date on which the request is made. The clinic does not have to provide a list when the information was:

- Used to provide treatment, payment and health care operations
- Provided to the patient
- Provided to employees responsible for the patient's care
- Provided to national security or intelligence
- Provided to correctional facilities or law enforcement officials
- Accessed prior to April 14, 2003.

The PHI Disclosure Log is used to provide a written account of times the patient's PHI was released. It includes the date of release, requesting entity, information provided, format of the information, purpose for disclosure or a copy of the written request, and the name and title of the person processing the release.

The Log is provided to the patient within 15 days of their request. The clinic will document the patient's request for the Log and the date the Log was given to the patient. A copy of the information released and the Log will be kept in the patient's medical chart.

Patient Right to Request Alternatives for Receiving PHI

Patients are allowed to request to receive communications of PHI from the covered health care provider by alternative means or at alternative locations. Examples are:

- Sending PHI to an alternative address for security reasons.
- Mailing the PHI in an envelope instead of using a postcard.
- Providing PHI to an alternative telephone number instead of the telephone number on record.

Patient Right to Request an Amendment of PHI

Patients are allowed to request to amend or supplement their medical record, in writing, using the Request for Amendment of the Medical Record form. The clinic can deny the request for the following reasons:

- PHI was not created by the organization.
- PHI is not part of the patient's designated record set.
- PHI is accurate and complete.
- PHI is not available to the patient for inspection as required by state and/or federal law (e.g. psychotherapy notes).

This information will be documented on the bottom of the Request for Amendment of the Medical Record form along with the signature of the staff person and processing date. The date of the response sent to the patient will also be recorded with the name of the staff person sending the response.

If the organization denies changes to the information, a letter will be sent to the patient explaining why and the patient's right to submit a written statement disagreeing with the denial to the clinic:
Schools of Occupational Therapy and Physical Therapy*, 1500 N. Warner #1030, Tacoma, WA, 98416-1030, (253) 879-3180.* Alternatively, the patient can submit a written statement to the Secretary of Health and Human Services (see Section 160.306 of the Federal Register Final Privacy Rule) to disagree with the denial.

If the organization agrees with the request to change the information, a letter will be sent to the patient acknowledging the decision and the process of notifying the individuals or organizations designated by the patient. A memo will be sent to the individuals or organizations identified by the patient with a copy of the completed Request for Amendment of the Medical Record form.

PHI DISCLOSURE LOG

Patient Name: ________________________________ Clinic Name: ____________________

Date of Release	Requesting Entity	Informatio n Provided	Format of Information	Purpose for Disclosure (or attach copy of request)	Release Processed By:	
					Name	Title

* *

FOR OFFICE USE ONLY:
Date patient requested PHI Disclosure Log: _______________
Copy of Log to patient on: _______________________________
By: ____

University of Puget Sound Schools of Occupational Therapy and Physical Therapy

REQUEST FOR AMENDMENT OF THE MEDICAL RECORD

Patient Name: ____ Date of Birth: _______________
Last First Middle

Address: ____
Street Address Apt. Number City State Zip Code

Phone: (Work) ____________________ (Home) __________________ (Cell) _____________________

After review of my medical record, I do not feel the original documentation is accurate for the following service dates: ____ and should be supplemented with clarifying information in the form of an addendum to my medical record. I understand that the physician or health care provider may or may not supplement my record with an addendum based on my request. I understand that my physician or other health care provider is not allowed to alter the original documentation in my record. I understand that my request for amendment will be made a permanent part of my medical record and will be sent with any future authorized medical record request for information.

I understand I have the opportunity to provide a statement of disagreement should my physician or health care provider deny my request.

Reason for amendment: ____

I request the following correction/amendment be made on my medical record:

____

____

____

I would like this amendment sent to the following individuals or organizations:

____

____

(Use back of form if needed)

____ ______________________
Signature of Patient or Personal Representative Date

* *

For Health Care Organization Use Only:
Date Received: __________________ ق Amendment Accepted ق Amendment Denied

If denied, check reason for denial:
ق PHI not created by this organization
ق PHI is not part of the patient's designated record set
ق PHI is accurate and complete
ق PHI is not available to the patient for inspection as required by state and/or federal law (e.g. psychotherapy notes)

Staff Signature: ______________________ Print Name & Title: ______________________________

Date: _________

Date response sent to Patient: _______ by____

Revised 12-2023; 01-2025; 08-2025

SAMPLE AMENDMENT DENIAL LETTER TO PATIENT

Date

Patient Name
Address

Dear _____,

Your request to amend your health information (see attached form) has been denied for the following reasons:

You have the right to submit a written statement disagreeing with the denial. If you wish to submit a statement of disagreement, use the following process:

[Include description, name, title, and phone number of person who handles statements of disagreement.]

Your request for an addendum will be made part of your permanent medical record and will be sent as part of the medical record in response to any authorized requests for your medical information.

You may also file a complaint with *[include regional complaint policy process].* You may also file a complaint with the Secretary of Health and Human Services (see Section 160.306 of the Federal Register Final Privacy Rule).

Sincerely,

SAMPLE AMENDMENT APPROVAL LETTER TO PATIENT

Date

Patient Name
Address

Dear _____,

Your request to amend your health information (see attached form), has been approved and we are in the process of notifying the individuals and/or organizations that you have identified.

In addition we have identified the following individuals and/or organizations that received your medical information. If you would like us to notify the individuals and organizations listed below, please sign, date, and return this statement and we will continue with the notification process.

_____
_____
_____
_____
_____
_____
_____
_____

I consent to the notification of the above individuals and organizations of my amendment to my medical information.

_____ _____
Patient Signature or Personal Representative Date

(Patient: Please return the signed letter to: _____)

Administrative Requirements

Privacy Officer

The Schools of Occupational Therapy and Physical Therapy has a designated Privacy Officer. This individual is responsible for all necessary HIPAA activities and for reviewing violations that may occur in the onsite clinics or community-based teaching clinic experiences.

Privacy Officer Job Description

General responsibilities include the development, implementation and oversight of standards, policies and procedures for the protection of health care privacy, confidentiality and security.

Specific duties include:

1. Serve as the central point of accountability within the organization for privacy and security related issues.
2. Create and implement a corporate privacy compliance program.
3. Develop and implement the policies and procedures for the organization, as required throughout the HIPAA privacy regulation, and for compliance with federal and state regulations that address health related information generally and the organization's privacy compliance program.
4. Recommend and carry out employee privacy training and education.
5. Coordinate all activities with privacy implications.
6. Coordinate as necessary with the organization's legal counsel information services and technology coordinator, personnel administrator and medical or other area leaders.
7. Monitor all the organization's products, services and systems to assure meaningful privacy practices.
8. Conduct privacy risk assessments and internal privacy audits.
9. Maintain documentation of privacy complaints and/or incidents (see Privacy Officer Complaint/Incident Log).
10. Identify areas where the entity can improve its privacy efforts.
11. Manage a privacy dispute and verification process.
12. Report to management on how the organization is dealing with privacy issues.
13. Keep employees abreast of new developments that affect them.
14. Maintain appropriate liaison with governmental and other officials responsible for privacy, confidentiality and security issues.
15. Maintain consistency, credibility and trust within and outside the organization.

Employee/Student Training

All students, faculty, staff and other members of our workforce are trained annually on the policies and procedures with respect to PHI required by HIPAA, as necessary and appropriate for the members of our workforce to carry out their function within our organization. Individuals in any of the categories listed above will sign a "Documentation of HIPAA Training and Confidentiality Agreement" form during orientation or initial training. (See Appendix C). This form will be retained by the HIPAA Privacy Officer for the duration of the individual's association with the University.

Students will read and sign the Safeguards to Protect PHI Contract (See Appendix D) at the beginning of each semester they are enrolled in the clinic. Upon completion of each semester, students will sign a statement indicating that they have removed all de-identified patient-related content from their personal computer and university account.

Internal Monitoring

Monitoring processes for detecting illegal collection, disclosure, or use of PHI by employees, students or contractors include the following: *Audits, spot checks, and copying of medical records by designated personnel only.*

Periodic internal audits will be conducted *each semester.* See Security Policies for specific information regarding audit procedures.

Complaints

Revised 12-2023; 01-2025; 08-2025

Employees, patients, or the public may file complaints regarding alleged violations of privacy using the following procedure:

1. Any complaint regarding the privacy of PHI is to be made in writing to:
   University of Puget Sound Schools of Occupational Therapy and Physical Therapy
   Attn: HIPAA Privacy Officer
   1500 N. Warner #1030, Tacoma WA 98416
   (253) 879-3281
2. Upon receipt of the complaint, the Privacy Officer will:
   - Document the complaint using date, time and name of person making the complaint on the "Privacy Officer Complaint/Incident Log.".
   - Investigate the complaint.
   - Document the resolution of the complaint and file in personnel file or medical record for seven (7) years.
   - Communicate the outcome of the complaint to the person filing the complaint.

Employee Sanctions

The University of Puget Sound Schools of Occupational Therapy and Physical Therapy will apply sanctions to employees and students violating our organization's privacy policies and procedures.

Employee discipline for privacy violations are determined by three levels of breach of privacy.

Level 1 Breach
- *Inadvertent breach of privacy (accidental/often due to lack of education or awareness).*
- *Examples: failing to log off a computer terminal or sharing passwords*
- *Options to address concern: verbal warning and mandatory re-education for first offense up to termination for repeated offenses.*

Level 2 Breach
- *Intentional breach without malice (accessing a patient record with no legitimate business purpose for doing so).*
- *Examples: accessing record of a friend or relative out of curiosity or releasing patient information inappropriately.*
- *Options to address concern: written warning for first offense up to termination for repeated offenses.*

Level 3 Breach
- *Intentional breach with malice (accessing a patient record with intent to use it for personal gain or to harm someone).*
- *Options to address concern: Termination for cause.*

Each episode of employee/student discipline for breaching the privacy policies and procedures of our organization will be documented and reported to the Privacy Officer. Documentation will include:
- *Name of employee*
- *Location of violation*
- *Date and time of violation*
- *Level of violation*
- *Disciplinary action taken*

HIPAA Violations and Enforcement

The Office of Civil Rights is responsible for enforcing the HIPAA Privacy and Security Rules. Failure to comply with HIPAA can result in monetary and/or criminal penalties.

HIPAA Violation	Minimum Civil Penalty	Maximum Civil and Criminal Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation with an annual maximum of $25,000 for repeat violations.	$50,000 per violation with an annual maximum of $1.5 million
Violation due to reasonable cause and NOT due to willful neglect	$1000 per violation with an annual maximum of $100,000 for repeat violations.	$50,000 per violation with an annual maximum of $1.5 million AND 1-5 years in prison
Violation due to willful neglect and corrected within the required time period	$1000 per violation with an annual maximum of $100,000 for repeat violations.	$50,000 per violation with an annual maximum of $1.5 million AND 1-5 years in prison
Violation due to willful neglect and NOT corrected within the required time period	$50,000 per violation with an annual maximum of $1.5 million	$250,000 per violation AND 10 years in prison

Mitigation
All covered entities must mitigate any harmful effect of a use or disclosure of PHI that is known to the organization. This duty extends to violation of internal policies and procedures, not just violations of the regulations.

The process for mitigating the effect of an unauthorized release of information by the clinic or any business associate includes:

1. The clinic is notified that PHI has been misused by an employee or business associate.
2. This information is communicated to the Privacy Officer.
3. If the information has been misused by an employee, the policy on employee sanctions is implemented.
4. If the information has been misused by a business associate, the clinic is to:
    - Investigate the misuse
    - Determine level of violation
    - Determine if violations repeated
    - Counsel the business associate on the misuse of PHI
    - Monitor the business associate to ensure violation has been remedied.
5. The University of Puget Sound Schools of Occupational Therapy and Physical Therapy reserves the right to terminate a business associate contract in the event that the violations continue despite counseling.

Whistleblowers
The University of Puget Sound Schools of Occupational Therapy and Physical Therapy will investigate allegations of misconduct by an employee/student or business associate for releasing PHI.

When employees/students or business associates report alleged violations, they must in good faith believe that the clinic has engaged in unlawful conduct, has violated professional or clinical standards, or the care, services or conditions provided by the clinic potentially endangers one or more patients, employees, or the public.

HIPAA prohibits the intimidation, threatening, coercion, discrimination against, or other retaliatory action against individuals for:

- Exercising their rights under HIPAA.
- Filing a complaint with the HHS Secretary.
- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing.

- Opposing any act or practice made unlawful by HIPAA Administrative Simplification, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA regulations.

Identity and Authority Verification

The procedure for verifying the identity and authority of a person requesting PHI, when the request is from a person who is not known to this organization requires at least one of the following:

1. Ask to see a badge or other proof of the identity of government officials.
2. Statement of the government officials and others regarding the legal authority for the activity.

The verification requirements of this provision are met if the University of Puget Sound Schools of Occupational Therapy and Physical Therapy relies on the exercise of professional judgment or acts on a good faith belief in making a use or disclosure under the circumstances listed above.

Provision for the Individual to Agree or Object

Some circumstances do not need an authorization of the individual to use or disclose PHI as long as the individual has received advance information delivered orally by the University of Puget Sound Schools of Occupational Therapy and Physical Therapy and the University of Puget Sound Schools of Occupational Therapy and Physical Therapy has received the individual's oral agreement or objection to the use or disclosure of the information. The individual must have an opportunity to agree to or prohibit or restrict the disclosure of PHI under the following circumstances:

1. To a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual regarding the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.
2. To notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.

Deceased Individuals

If an executor, administrator, or other person has lawful authority to act on behalf of a deceased individual or of the individual's estate, the University of Puget Sound Schools of Occupational Therapy and Physical Therapy must treat such a person as a personal representative under HIPAA Administrative Simplification, with respect to PHI that is relevant to such personal representation.

Personal Representatives

A person who has the lawful authority to act on behalf of an adult individual in making
health care decisions will be treated as would the individual with respect to using or disclosing that individual's PHI. This provision also applies when the individual is an emancipated minor.

Marketing

PHI may not be used or disclosed for marketing purposes without obtaining proper authorization from the individual. However, authorization is not required when the use or disclosure of the PHI is used to make a marketing communication to an individual that:

- Occurs in a face-to-face encounter with the individual.
- Concerns products or services of nominal value.
- Concerns the health-related products and services of *[insert name of org.]* or of a third party and the communication meets certain applicable conditions described under the regulations. PHI may be disclosed for purposes of such communications only to a business associate that assists the covered entity with such communications.

APPENDIX A – Documentation of HIPAA Training and Confidentiality Agreement

School of Occupational Therapy and Physical Therapy
STUDENT FACULTY STAFF
Documentation of HIPAA Training and Confidentiality Agreement

Revised 07/15/2019; Reviewed 07/1/2020

The University of Puget Sound Schools of Occupational Therapy and Physical Therapy have a legal and ethical responsibility to protect the privacy of all patients and to protect the confidentiality of their health information. Further, the Schools of Occupational Therapy and Physical Therapy must also assure that their employees, students, independent contractors, and business associates keep protected health information confidential.

Patients/clients have a legal right to privacy concerning their medical records. It is the obligation of the University of Puget Sound School s of Occupational Therapy and Physical Therapy to uphold that right. For this reason, no member of the university to whom medical records or patient information is available may in any way violate this confidentiality except with written consent of the patient and in accordance with The University of Puget Sound Schools of Occupational Therapy and Physical Therapy HIPAA Policies and Procedures for Privacy and Security, federal rules and regulations, and Washington State laws governing privacy and confidentiality.

- I agree that I will only access records for school/employment related and "need to know" purposes and that I will not disclose the content of those records apart from the requirements of the school or my employment or other affiliation.

- I acknowledge that a breach of confidentiality may result in termination of my enrollment in the School of Occupational Therapy and Physical Therapy or my employment/affiliation at the university as well as additional disciplinary action applicable by University policy and/or Federal law.

- I have read the above statement and I agree to abide by it.

- I certify that I have received training on the HIPAA rules by watching the video at https://www.youtube.com/watch?v=s9znUYvVO4A and reviewed this entity's HIPAA policies & procedures in the University of Puget Sound Onsite Clinics Operations Manual.

_____ _____
Printed Name Date

_____
Signature

Revised 12-2023; 01-2025; 08-2025

APPENDIX B – HIPAA Training and Confidentiality Agreement Clinical Instructors

School of Occupational Therapy and Physical Therapy
Confidentiality Agreement & Documentation of HIPAA Training
CLINICAL INSTRUCTORS
Revised 12/2017; Reviewed 07/2019; 7/2020

The University of Puget Sound Schools of Occupational Therapy and Physical Therapy have a legal and ethical responsibility to protect the privacy of all patients and to protect the confidentiality of their health information. The University of Puget Sound Schools of Occupational Therapy and Physical Therapy must also assure that its employees, students, independent contractors, and business associates keep protected health information confidential.

The patient has a legal right to privacy concerning his/her medical record. It is the obligation of the University of Puget Sound Schools of Occupational Therapy and Physical Therapy to uphold that right. For this reason, no member of the university to whom medical records or patient information is available may in any way violate this confidentiality except with written consent of the patient and in accordance with The University of Puget Sound Schools of Occupational Therapy and Physical Therapy policies, Federal rules and regulations, and the Washington State laws governing privacy and confidentiality.

- I agree that I will access records only for school/employment and 'need to know' situations and that I will not disclose the content of those records apart from the requirements of the school/employment.
- I acknowledge that a breach of confidentiality may result in termination of my enrollment in the School of Occupational Therapy and Physical Therapy plus additional disciplinary action as appropriate by University policy and/or Federal law
- I have read the above statement and agree to abide by it.
- I certify that I have received training on the HIPAA privacy and security rules either by watching the video at https://www.youtube.com/watch?v=s9znUYvVO4A **or** training offered by my employer outside of the university* *within the last year,* and that I have reviewed and agree to abide by this entity's HIPAA policies & procedures in the University of Puget Sound Onsite Clinics Operations Manual.

_____
Printed Name

_____ _____
Signature Date

*If HIPAA training was completed for an outside employer, certification of the training provided must be attached to this form.

APPENDIX C – Student PHI Contract

Safeguards to Protect PHI
Contract
Revised 12/2017; Reviewed 7/2019; 7/2020

Students who have contact with patients who are being seen in any of the onsite clinics on campus or in the community as part of a community-based teaching clinic must abide by the following regulations related to the protection of Protected Health Information (PHI). The information below comes from the federal regulations regarding the protection of PHI as well as the HIPAA Policies and Procedures that are currently in place for the Schools of Occupational Therapy and Physical Therapy at the University of Puget Sound. This contract is in addition to, not in replacement of the Confidentiality Agreement that students in both programs are required to sign after receiving the requisite training.

Oral Communications

Oral communications must occur freely and quickly in treatment settings. However, reasonable safeguards must be taken to protect oral PHI. Examples of safeguards include, but are not limited to

1. lowering voices when in open patient areas
2. moving to a private location to have conversations
3. closing doors

These safeguards do not guarantee the privacy of PHI from any and all potential risks, but are the reasonable precautions taken to minimize the chance of inadvertent disclosures to persons who may be nearby. NOTE: The chart storage area in WEY 107 is not considered a private location due to the number of individuals who potentially need access to the charts at any time during clinic.

Telephone Conversations

Students and/or clinical instructors who have telephone conversations in which a person's PHI is discussed must have those conversations in a private area where the conversation cannot be overheard. The phone in WEY 105 is designated specifically for that purpose. Examples of such communication include conversations with physicians, DME suppliers, pharmacies, caregivers, etc. This may mean asking to use a faculty member's office or an unoccupied room and closing the door for privacy. When phoning physicians, DME providers, pharmacies, etc. regarding a patient or client; please identify yourself by name and clinical affiliation (i.e. the respective onsite clinic at the University of Puget Sound). Do not ask the clinic to return the call to your personal cell phone. Instead use the onsite clinic phone number (253) 879-3180 for PT and (253) 879-3499 for OT. If you leave a message with one of the types of businesses listed above about a specific patient or client, it is appropriate and necessary for you to identify the person by name and you may also need to leave detailed PHI. This is <u>not</u> a violation of HIPAA regulations.

Telephone messages for students or clinical instructors that are left with the office assistant will not contain identifying information such as a patient's name or other PHI that can be directly linked to an individual.

Faxes

Documents containing PHI should be sent via fax transmittal if at all possible. Fax cover sheets are used with all fax transmittals and confirmation sheets are produced to ensure accurate transmittal. Faxes should be given to the office assistant with the cover sheet in place. A copy of the original document and the fax cover sheet will be returned to the person requesting that the fax be sent as soon as it has been sent.

Computer Screens & Appointment Schedules

Computer screens will be turned away from view by the public including patients, patient's families and visitors. Students must log off of the computer when they are not using it. Appointment schedules for the day are placed in a secure location for student therapist or clinical instructor access but are not visible to the general public.

Medical Records

Medical records of current patients are stored securely out of sight in Weyerhaeuser Hall room 107 and in WebPT™ for PT Onsite Clinic and on the UPS HIPAA compliant Google Drive™ for OT. The following categories of employees/students may be permitted access to these medical records:

- physical therapy or occupational therapy students
- Clinical Instructors of physical therapy or occupational therapy students
- Faculty clinic coordinator for the respective program
- Front office personnel
- Ancillary staff such as clinic aides
- Faculty members of the School of Occupational Therapy and Physical Therapy

Patient medical records/charts will not be left open and unattended in patient access areas. If the therapist is not working directly with the chart, it will be closed and turned over or covered with a piece of blank paper. Charts in the bins in room 107 must have the names turned toward the wall.

Medical records are not to be taken out of Weyerhaeuser Hall by therapists/students under any circumstances. Family, friends, and/or visitors may not have access to the information in the medical record at any time.

VI. Documentation

Documentation of all Physical Therapy patient/client encounters will be done in WebPT™. WebPT may only be accessed with a computer or personal device that has been encrypted. **Failure to use a device that has been encrypted will result in revocation of access to WebPT.**

Documentation of all Occupational Therapy patient/client encounters will be done in the UPS HIPAA compliant Google Drive. Client information on the UPS HIPAA compliant Google Drive may only be accessed with a computer or personal device that has been encrypted. **Failure to use a device that has been encrypted will result in revocation of access to the UPS HIPAA compliant Google Drive.**

PHI such as patient evaluation and treatment data may be stored on a data transport device such as an encrypted jump drive provided that all of the following conditions are met:

- The data transport device must be encrypted.
- The patient's name cannot appear on any of the data stored.
- The patient's name should be added to the electronic note immediately before the note is printed and must be removed from the electronic device immediately after the print job is completed.
- All PHI that is stored on a data transport device must be removed as soon as it is no longer needed in electronic form and immediately upon conclusion of the onsite teaching clinic.

Any documents containing identifiable PHI must be shredded prior to disposal. Documents that need to be shredded should be placed in the locked shred bins in WEY 105 or 107.

My signature below indicates that I have read and that I agree to all of the regulations above. I understand that this contract does not supersede the Confidentiality Agreement that I signed following training on HIPAA Policies and Procedures. I further understand that failure to abide by these regulations may impact my standing as a student or employee of the university.

_____	_____
Printed Name	Signature
_____	_____
Title or Designation	Date

Revised 12-2023; 01-2025; 08-2025

APPENDIX D – Consent for Photography

Consent for Photography and Authorization for Use and Disclosure

Revised 04/2021

Patient Name _____ Date _____

I hereby consent to be photographed while receiving care in the Occupational Therapy or Physical Therapy Onsite Clinic at the University of Puget Sound. The term "photograph" includes video or still photography, in digital or any other format, and any other means of recording or reproducing images.

I hereby authorize the use of the photograph(s) by, or disclosure of the photograph(s) to:

_____*(Persons/Organizations authorized to receive the information)*

_____*(Address—street, city, state, zip code)*

I hereby authorize the use or disclosure of the photograph(s) for the following uses or purposes _____(*describe permitted uses*).

I consent to be photographed and authorize the use or disclosure of such photograph(s) in order to assist treatment and to support educational goals. I hereby waive any right to compensation for such uses by reason of the foregoing authorization.

This Authorization expires on _____*(insert date)*:

Upon expiration of this Authorization, the University of Puget Sound Schools of Occupational Therapy or Physical Therapy will not permit further release of any photograph but will not be able to call back any photographs or information already released.

I understand that I may request cessation of filming or recording at any time. I may rescind this Authorization up until a reasonable time before the photograph is used, but I must do so in writing and submit it to the following address:

University of Puget Sound
Schools of Occupational Therapy and Physical Therapy
1500 N Warner St CMB 1030
Tacoma, WA 98416

_____Signature
(patient/spouse/legal guardian)

_____ Print Name
(patient/spouse/legal guardian)

If signed by someone other than patient, indicate relationship: _____

Revised 12-2023; 01-2025; 08-2025

HIPAA Security Policy Manual

Release Date January 2016
Revised April 2016
Revised April 2017
Revised December 2017
Revised May 2018
Revised July 2019
Revised July 2020
Revised 2021, 2022
Revised December 2023

Revised 12-2023; 01-2025; 08-2025

TABLE OF CONTENTS

Section 1: HIPAA Security Rule Summary

1.1 ***Overview***

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information (ePHI).

The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

1.2 ***HIPAA Hybrid Entity Designation***

The University of Puget Sound is considered a Hybrid Entity under the Health Insurance Portability and Accountability Act (HIPAA).

A single legal entity that otherwise qualifies as a hybrid entity must designate a component or combination of components as its HIPAA Health Care Components in accordance with 45 C.F.R. §§ 164.103 and 164.105(a)(2)(iii)(D). A HIPAA Health Care Component is a component of the single legal entity that would meet the definition of a HIPAA Covered Entity if it were a separate entity; or an office within the Hybrid Entity that accesses Protected Health Information of an office that is a Health Care Component for the purpose of providing services to the Health Care Component.

The University of Puget Sound has identified the following HIPAA Health Care Components:

- The Human Resources Department to the extent that it performs covered functions as the administrator of the self-funded group health plans that the university makes available to the employees.
- The School of Physical Therapy (PT) to the extent that it provides physical therapy services to members of the community who are not students at the university.
- The School of Occupational Therapy (OT) to the extent that it provides occupational therapy services to members of the community who are not students at the university.
- The School of Education to the extent that it provides mental health services to members of the community who are not students at the university.

The policy and procedure elements of this policy manual apply to the hybrid entity components of the university noted above, not to the University of Puget Sound in its entirety.

1.3 ***Definition of PHI / ePHI***

Protected Health Information. The 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. The Privacy Rule calls this information "protected health information (PHI)."
"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present, or future physical or mental health or condition

- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

A data set may be considered "de-identified" and thus no longer PHI if it has 18 identifiers removed. The department of Health and Human Services has provided guidance on this process here.

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

Electronic Protected Health Information. The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule here. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The HIPAA Security Rule calls this information "electronic protected health information" (ePHI). The Security Rule does not apply to PHI transmitted orally or in writing.

1.4 Security Rule Goals and Objectives

The security standards noted in the HIPAA Security Rule include the general requirements all covered entities must meet. HIPAA establishes flexibility of approach, identifies standards and implementation specifications (both required and addressable), outlines decisions a covered entity must make regarding addressable implementation specifications, and requires maintenance of security measures to continue reasonable and appropriate protection of electronic protected health information.

In 45 CFR 164.306(a) the HIPAA Security Rule requires that each covered entity must:

- Ensure the confidentiality, integrity and availability of ePHI that it creates, receives, maintains or transmits
- Protect against any reasonably anticipated threats and hazards to the security or integrity of ePHI
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule (i.e. data breaches).

1.5 Required and Addressable Components of the Rule

Within the Security Rule sections are standards and implementation specifications. Each HIPAA Security Rule standard is required. A covered entity is required to comply with all standards of the Security Rule with respect to all ePHI.

Many of the standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard. **Implementation specifications are either required or addressable**. However, regardless of whether a standard includes implementation specifications, covered entities must comply with each standard.

A **required** implementation specification is similar to a standard and a covered entity must comply with it.

For **addressable** implementation specifications, covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity's environment. In general, after performing the assessment, a covered entity decides if it will implement the addressable implementation specification; implement an equivalent alternative measure that allows the entity to comply with the standard; or not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment. Covered entities are required to document these assessments and all decisions.

Often times implementation specifications may not be detailed enough to provide appropriate guidance to a covered entity or security practitioner. In these cases, guidance will be sought from standards documentation produced by the National Institute of Standards and Technology (NIST). NIST is a non-regulatory federal agency within the U.S. Department of Commerce.

The Computer Security Division (CSD), a component within NIST's Information Technology Laboratory (ITL), provides standards and technology to protect information systems against threats to the confidentiality of information, the integrity of information and processes, and the availability of information and services in order to build trust and confidence in IT systems.

CSD develops and issues standards, guidelines, and other publications such as the Federal Information Processing Standards (FIPS) and Special Publications (SP) 800-series documentation which can be used for guidance by covered entities such as the University of Puget Sound when building and maintaining an information security program.

Section 2: Administrative Safeguards

2.1 Overview

This section describes administrative safeguards required by HIPAA. Administrative Safeguards are defined in the Security Rule (45 CFR 164.304) as the "administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

This section covers the pertinent Administrative Safeguards Policies for the university, particularly in the areas of security management, security responsibility, workforce security, information access management, awareness & training, incident response, contingency planning, periodic evaluation, and business associate relationships.

2.2 Security Management Process (45 CFR § 164.308(a)(1)(i))

The University of Puget Sound will implement a security management process which includes policies and procedures to prevent, detect, contain and correct security violations. The policy statements governing security management related to the HIPAA Security Rule at the university are contained within this document. Departmental procedures that provide operational activities supporting these policies will be created by their respective schools and departments.

Security Management at the university will include at a minimum the following disciplines or activities:

i. Risk Analysis (45 CFR § 164.308(a)(1)(ii)(A))

The University of Puget Sound will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information. The risk analysis will consider the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the university's information systems and the information they process, store, or transmit. The risk analysis should include the following aspects:

1. Identify each system the university staff accesses, and define the scope of the risk analysis based on how electronic media that contains ePHI is used.
2. Identify the vulnerabilities, risks, or threats to the security of ePHI within the systems.
3. Evaluate the impact of such vulnerabilities, risks, or threats to the systems.
4. Evaluate the effectiveness of the current security controls in place.
5. Determine the probability of a vulnerability breach or likelihood of a risk or threat occurring.
6. Recommend additional controls if needed, and develop and implement plan of action for adding such controls.
7. Document the risk assessment results.

The university security official or designee documents and maintains risk assessment results in a risk assessment report. The report will be reviewed and updated annually, or whenever there are significant changes to the information systems environment (including the identification of new threats and vulnerabilities) or when other conditions arise that may impact the secure operation of the system or process.

ii. Risk Management (45 CFR § 164.308(a)(1)(ii)(B))

The University of Puget Sound will implement a security management program sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 CFR 164.306(a).

In deciding which security technologies or techniques to use, the university will use the flexible approach provided in the HIPAA Security Rule and take into account the following factors:

1. The size, complexity, and capabilities of the university.
2. The university's technical infrastructure, hardware, and software security capabilities.
3. The costs of security measures.
4. The probability and criticality of potential risks to electronic protected health information.

In addition to improving the security of university systems, the risk management program will be used to discover risks and prioritize remediation efforts, thereby maximizing the effectiveness of a finite technology budget. Detailed risk management recommendations are available in NIST Special Publication 800-30.

iii. Sanction Policy (45 CFR § 164.308(a)(1)(ii)(C))

The University of Puget Sound will apply sanctions against workforce members who fail to comply with security policies and procedures related to the protection of ePHI. Workforce members may include employees, contractors, volunteers, students, etc. as deemed appropriate by the university. The sanction process will include corrective action up to and including termination of the workforce member's relationship with the

university under procedures specified by the Student Integrity Code, Staff Policies and Procedures, and the *Faculty Code*.

The university reserves the right, at its sole discretion, to accelerate sanctions, repeat sanctions, skip sanctions, or impose other sanctions, from time to time, based on the severity and nature of each security violation.

iv. Review of Information Systems (IS) Activity Records (45 CFR § 164.308(a)(1)(ii)(D))

Unauthorized prying, peering, or snooping into any individual's ePHI, is unacceptable and grounds for sanctions, regardless of the relationship between the university workforce member and the individual, and regardless of the individual's public or private status.

The University of Puget Sound will regularly review records of information systems activity such as audit logs, access reports, and security incident tracking reports. The records will be examined for indications of inappropriate or unusual activity, and if found, such activity will be investigated, and appropriate sanctions applied. The level of audit review, analysis, and reporting will be adjusted based on risk to the information system or university as an organization.

AUDIT PROCEDURE FOR PHYSICAL THERAPY:
The University of Puget Sound will review 10 percent of the total census of patients who are actively receiving Physical Therapy (PT) services twice a month when clinic is in operation using the following procedures:

1. Equal numbers of patients being seen for orthopedic, neurologic and pediatric conditions will be selected.
2. The medical records will be reviewed to determine who has accessed those records.
3. Those who are authorized to access records include the clinical instructor (therapist of record), the student physical therapist or student occupational therapist who is providing the care and if applicable, the clinical instructor from the opposite discipline who is also responsible for providing care to the patient.
4. The identities of individuals who have accessed the records will be compared to those who have authorization to do so and any deviations will be investigated.

AUDIT PROCEDURE FOR OCCUPATIONAL THERAPY:

Paper health records

Paper health records for 10% of all clients receiving care in the OT clinics are randomly selected for review every two weeks when clinics are in session. The review consists of identifying the student and clinical instructor (CI) team who are working with that client and any administrative staff who entered information into the record during the past two weeks. Any access by individuals who are not part of the student-CI team or clinic administrative staff will be further investigated for incidents of unauthorized access.

Electronic health records

Electronic health records for 10% of all clients receiving care in the OT clinics are randomly selected for review every two weeks when clinics are in session. The review consists of identifying the student and clinical instructor (CI) team who are working with that client and any administrative staff who entered information into the record during the past two weeks. Any access by individuals who are not part of the student-CI team or clinic administrative staff will be further investigated for incidents of unauthorized access.

2.3 ***Assigned Security Responsibility (45 CFR § 164.308(a)(2))***

The University of Puget Sound has assigned the role of HIPAA Security Official to the Chief Information Officer (CIO). The Security Official is responsible for the development and implementation of the policies and procedures that support compliance with the HIPAA Security Rule.

2.4 ***Workforce Security (45 CFR § 164.308(a)(3)(i)) & Information Access Management (45 CFR § 164.308(a)(4)(i))***

The University of Puget Sound will ensure that appropriate members of its workforce have access to ePHI as needed. This responsibility includes providing access when it is needed as part of healthcare treatment, payment, or operations, and also prohibiting access when it is not needed or not appropriate.

In support of this effort, the university will appropriately document and authorize access to ePHI through departmental procedures which support each system or application in use (See below). University management will authorize and supervise access (45 CFR § 164.308(a)(3)(ii)(A)) to ePHI for staff and students by ensuring access is granted only after the completion of a successful background check. The university will also ensure appropriate access is maintained by periodically reviewing access (45 CFR § 164.308(a)(3)(ii)(B)) through an entitlement review process.

If the relationship between a member of the workforce and university terminates, or if a review of access rights shows that the workforce member's access to ePHI is not appropriate, the university will adjust or terminate the user's rights to ensure the access is updated to the appropriate level (45 CFR §164.308(a)(3)(ii)(C)).

Access rights modifications/deletions are typically performed through standard procedures, however exigent circumstances may occasionally require that access is terminated immediately upon email or phone notification from a manager to the system administrator or manager responsible for access to the resource.

PROCESS FOR PHYSICAL THERAPY:

Access to electronic health records (WebPT™ application) will be authorized and reviewed, changed or terminated by the clinic director for PT as follows:

1. The clinic director identifies all students and clinical instructors who will be responsible for providing care in the onsite clinic.
2. A roster of these individuals will be sent to WebPT to be entered into the system for both the training platforms and the actual clinic platforms by WebPT.
3. Access is granted to the training platform for the duration of the academic program and to the clinic platform for a single semester only. At the end of each semester, the clinic director will inactivate access for all students and clinical instructors from the clinic platform. Individuals who will need to have access for subsequent semesters will be reactivated by the clinical directors when needed.

PROCESS FOR OCCUPATIONAL THERAPY

Access to electronic health records in the UPS HIPAA compliant Google Drive will be authorized and reviewed, changed or terminated by the clinic coordinators as follows:

4. The clinic coordinators identify all students and clinical instructors who will be responsible for providing care in the OT teaching clinics.
5. The OT Clinic Assistant, under the supervision of the clinic coordinators, is responsible for entering these individuals into client records in the UPS HIPAA compliant Google Drive.

6. Access is granted for a single semester only. At the end of each semester, the clinic coordinators and/or OT Clinic Assistant will inactivate access for all students and clinical instructors from the clinic platform.

2.5 ***Security Awareness and Training*** ***(45 CFR § 164.308(a)(5)(i))***

The University of Puget Sound will implement a mandatory security awareness and training program for members of its workforce, including management, who access ePHI. The training format will include a standard course that covers information security best practices and periodic awareness reminders in support of HIPAA. The content of the training and awareness material will include, at a minimum, the following topics (45 CFR § 164.308(a)(5)(ii)):

- Protection from Malicious Software – describing procedures and actions that members of the workforce can take for guarding against, detecting, and reporting malicious software
- Log-in Monitoring – describing procedures used to monitor login and system activity and report discrepancies
- Password Management – describing procedures and best practices for creating, changing and safeguarding passwords

All awareness and training material will be retained for at least six years from the last date of use to serve as an artifact of the content presented to the workforce.

2.6 ***Security Incidents*** ***(45 CFR § 164.308(a)(6)(i))***

The University of Puget Sound will develop and maintain an incident response plan which will contain policies and procedures to address security incidents. The plan will include procedures for addressing main types of incidents:

- Denial of Service / System Outage
- Malicious Code
- Unauthorized Access
- Inappropriate Usage

The procedures will follow a standard three-phase methodology of incident detection and analysis; containment, eradication and recovery; and post-mortem analysis. The post-mortem analysis should include a feedback loop into other university policies, procedures, standards, systems, etc. so that needed changes can be made to prevent incidents from re-occurring.

The incident response plan(s) will include guidance on how to:

- Identify and respond to suspected or known security incidents
- Mitigate, to the extent practicable, harmful effects of security incidents that are known to the university.
- Document the incidents and their outcomes so that a complete understanding of the incident's cause and effect is known and recorded

The university HIPAA Security Official will be notified of all computer security incidents. Where systems are hosted and maintained by third parties, the university may defer to the third party's incident response procedures.

2.7 ***Contingency Planning*** ***(45 CFR § 164.308(a)(7))***

The University of Puget Sound uses a third-party hosted medical record application and relies upon the third party's contingency planning procedures to ensure data is available in the event of an emergency or other

occurrence (e.g. fire, vandalism, system failure, natural disaster) that damages systems that contain ePHI. Contingency plans are designed to enable operations to continue or recover during periods of short term system unavailability and long term system downtime. The contingency plans in place at the third party provider contain at a minimum, the following components:

- A Data Backup Plan that will establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information
- A Disaster Recovery Plan that will establish (and implement as needed) procedures to restore any loss of data
- An Emergency Mode Operation Plan that will establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode

These third party plans will be supported by at least the following activities:

- An Applications and Data Criticality Analysis, which will assess the relative criticality of specific applications and data. When assessing applications, the underlying infrastructure, servers, network, storage equipment required to run the application must also be taken into consideration.
- Testing and Revision procedure(s) that describe periodic testing and revision of contingency plans. Periodic testing results should be examined so that process improvements can be gleaned from the activity and implemented by technology staff.

Contingency planning documentation and activities specific to the university may be maintained by individual schools or departments or managed jointly with Technology Services. Technology Services does not maintain ePHI records.

2.8 ***Evaluation*** ***(45 CFR § 164.308(a)(8))***

The University of Puget Sound will perform periodic technical and non-technical evaluations, based initially upon the HIPAA Security Rule, and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information. The goal of the evaluation process is to establish the extent to which the university's security policies and procedures meet the requirements of the HIPAA Security Rule and protect ePHI.

This evaluation may be performed by internal staff or external consultants. The information security program at the university will be adjusted as needed to comply with regulations and to provide reasonable and appropriate protection of ePHI.

2.9 ***Business Associates*** ***(45 CFR § 164.308(b)(1))***

In general, a HIPAA business associate is a person or entity other than a member of the University of Puget Sound's workforce that performs functions or activities on the university's behalf, or provides specified services to the university that involve the use or disclosure of protected health information. A business associate may also be another HIPAA covered entity.

The university may permit a business associate to create, receive, maintain, or transmit electronic protected health information on its behalf. Such arrangements will only be permitted if the university obtains satisfactory

assurances, in accordance with 45 CFR § 164.314(a) of the HIPAA Security Rule, that the business associate will appropriately safeguard the information.

Prior to sharing or providing access to University of Puget Sound ePHI, the university will document the satisfactory assurances through a written contract, or other arrangement with the business associate, that meets the applicable requirements of 45 CFR § 164.314(a).

Section 3: Physical Safeguards

3.1 ***Overview***

This section describes physical safeguards required by HIPAA. Physical Safeguards are defined in the Security Rule (45 CFR 164.304) as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

This section covers the pertinent Physical Safeguards Policies for the university, particularly in the area of facility security, workstation use, and electronic media control.

3.2 ***Facility Access Controls (164.310(a)(1))***

The University of Puget Sound will limit physical access to its electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. The university will safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

The university will:

- Develop a Facility Security Plan which will include procedures to safeguard the facilities and the equipment therein from unauthorized physical access, tampering, and theft. (164.310(a)(2)(ii)) The plan should include:
    - Appropriate measures to provide physical security protection for ePHI.
    - Documentation of the facility inventory, as well as information regarding the physical maintenance records and the history of changes, upgrades, and other modifications.
    - Points of access to the facility and existing security controls in place to protect them.

- Implement access control and validation procedures (164.310(a)(2)(iii)) to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs containing ePHI. To support these requirements, visitors will be monitored and third party vendors who access university ePHI will have their identities confirmed and a Business Associate Agreement in place.

- Establish (and implement as needed) contingency operations procedures (164.310(a)(2)(i)) as noted in section 2.7 that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.

- Implement maintenance policies and procedures (164.310(a)(2)(iv)) to document repairs and modifications to the physical components of the office in regards to security (for example, hardware, walls, doors and locks). Repairs and improvements related to security will be logged.

PROCESS:

Physical access to Weyerhaeuser Hall is granted based on the following procedures:

1. Clinical Instructors are issued keys and ID card swipe access to the clinic space by Security Services once they have signed and returned their faculty contracts.

2. Keys are returned to Security Services at the end of each semester expect for those Clinical Instructors who have ongoing contracts with the university.
3. Students are granted ID card swipe access to limited clinic spaces at the beginning of each academic year. The access is limited to those spaces that a student will need to access either during clinic or after hours.
4. The relevant program director for PT and OT sends a roster of students who need access to Security Services at the beginning of each semester.
5. Card swipe access is removed by Security Services the day after the last day of final exams at the end of each semester.

3.3 ***Workstation Use and Security (164.310(b)&(c))***

The University of Puget Sound will implement appropriate policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

The university will also implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. Safeguards include encryption of all university computers in Weyerhaeuser Hall, privacy screens and locking screen savers.

In support of this policy, the university will identify the types and functions of different classes of workstations, analyze the physical surroundings of workstations to ascertain if physical access to the workstations is appropriate, and take needed steps to mitigate risks discovered.

WebPT and users are required to access these platforms via an encrypted device. The policy and procedures regarding encryption of personal devices are in Addendum B.

Paper documents containing PHI can be uploaded to WebPT as an eDOC using the scanner that is located in Weyerhaeuser Hall room 105 only. The procedure for using the scanner in the most secure manner is as follows:
Log onto WebPT via Internet Explorer on the encrypted computer in WEY 105 and select the patient record of interest. Click on eDOC in the Patient Information section. Name the document to be scanned, e.g., Referral, Consent Form, etc. Place the document face down on the scanner. Click "Quick Scan". Verify that the document scanned correctly. Remove the paper document from the scanner and place it in the shred bin.

3.4 ***Device and Media Controls (164.310(d)(1))***

The University of Puget Sound will implement procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of the campus facilities, and the movement of these items within the campus. The procedures will address, at a minimum, the following requirements:

- Final disposition: The university will implement procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored.
    - Hard disks will be destroyed before leaving university facilities or will be destroyed by a vendor who provides a certificate of destruction for the media.
    - Backup tapes containing ePHI will be destroyed before leaving university facilities or will be destroyed by a vendor who provides a certificate of destruction for the media.

  - Any other storage media will be destroyed or sanitized with a wiping method which renders ePHI unreadable and unrecoverable.

- Reuse: The university will implement procedures describing the method used for removal of ePHI from electronic media before the media are made available for reuse in an area not approved for access to ePHI.

- Hardware accountability: The university will maintain a record of the movements of hardware and electronic media containing ePHI and any person responsible therefore.

- Backup and storage: The university or, designated third party vendor will create a retrievable exact copy of ePHI, when needed, before movement of equipment.

Section 4: Technical Safeguards

4.1 Overview

This section describes technical safeguards required by HIPAA. Technical Safeguards are defined in the Security Rule (45 CFR 164.304) as the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

This section covers the pertinent Technical Safeguards Policies for the university, particularly in the area of access control, audit controls, data integrity, authentication, and transmission security. Where the safeguards noted are controlled by a third party vendor, such as a hosted application provider, the university will rely upon the vendor's HIPAA safeguards.

4.2 Access Controls (164.312(a)(1))

v. The university will implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in section 2.4.

vi. The access controls in place at the university will have the following minimum functions or features:

- Each user will have a unique user identifier suitable for tracking user identity.
- The university will establish, maintain and implement as-needed procedures for obtaining access to necessary ePHI during an emergency.
- Electronic sessions will terminate after a predetermined time of inactivity.
    - This time period may vary depending upon mitigating factors such as proximity to public view, physical security of the system, sensitivity of the data on the screen, etc. but in no case will it exceed 5 minutes.
- Encryption will be used wherever deemed appropriate to protect ePHI from unauthorized disclosure and alteration.

4.3 Audit Controls (164.312(b))

vii. The Physical Therapy program uses a web-based electronic health record system (WebPT) which logs user activity related to the use of electronic protected health information. The director of the PT Onsite Clinic reviews the log data on a regular basis. The Occupational Therapy program uses the UPS HIPAA compliant Google Drive. See audit process described in Section 2.2 above.

4.4 Data Integrity and Transmission Security (164.312(c)&(e))

viii. The university will implement procedures to protect electronic protected health information from improper alteration or destruction. The university will also implement

electronic mechanisms to ensure ePHI has not been accessed, altered, or destroyed in an unauthorized manner while at rest or in transit. The university will employ cryptographic mechanisms to prevent unauthorized disclosure of information during storage and/or transmission where appropriate.

ix. To support these requirements, communicating ePHI over standard (non-encrypted) channels such as email, texting, or other insecure medium is prohibited.

x. When implementing encryption technologies The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet the cryptographic standard described in the HIPAA Security Rule.

- Valid encryption processes for data at rest are consistent with NIST Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices.
- Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications:
  - 800–52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; or
  - 800– 77, Guide to IPsec VPNs; or
  - 800–113, Guide to SSL VPNs, or
  - others which are Federal Information Processing Standards (FIPS) 140–2 validated.

xi. The university will use the aforementioned documentation as guides when examining and deploying technology solutions used to protect ePHI.

*4.5 **Person or Entity Authentication** (164.312(d))*

xii. The university will implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. This will be accomplished through background checks which verify the identity of members of the workforce. User actions will further be authenticated through procedural and technical controls that ensure users logging into systems use a unique identifier and confidential password so that all activities performed under the user ID are properly attributable to the person to whom the user ID is assigned.

xiii. The minimum password requirements for user accounts in WebPT which access ePHI include the following:

- A minimum of eight characters
- Passwords must contain at least 3 of the following: one Uppercase and/or one lower case alphabetic character, one numeric character (0 through9 and one special character
- Passwords will expire at least every 90 days

Section 5: Data Breach Notification

5.1 ***Overview***

xiv. The HIPAA Omnibus Final Rule, effective September 23, 2013, expanded the scope of HIPAA to include notification in the event of a security incident resulting in an impermissible use or disclosure of PHI. Washington State has a similar statute for personally identifiable information (PII).

xv. The data breach section of HIPAA is known as the Data Breach Notification Rule (45 CFR §§ 164.400-414) and requires HIPAA covered entities to provide notification following a breach of unsecured protected health information. The Department of Health and Human Services has provided guidance on protecting PHI through proper encryption or destruction methodologies. If PHI is protected via one of the methods mentioned, it is not subject to the Breach Notification Rule.

In addition to HIPAA, Washington State statutes (RCW 19.255.010 and RCW 42.56.590) address data breach notification requirements for organizations that retain personally identifiable information (PII) on Washington residents, if there is a breach of unsecured PII. A breach of secured PII is generally not required to be reported unless the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person. The State of Washington defines "secured" as *encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.*

The Data Breach Notification Rule applies to physical, verbal, and electronic forms of PHI/PII. For potential breaches of unsecured PHI or PII, the university policy is described in the sections below.

5.2 ***Potential Breach Discovery and Analysis***

xvi.

Based on the information collected, the university will perform a risk assessment to determine the risk that the unsecured PHI/PII was compromised by the impermissible use or disclosure. For PHI, this analysis will include a determination of the existence of any exclusionary conditions noted in HIPAA which, if present, would preclude the incident from becoming a data breach:

- Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

- Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

- A disclosure of protected health information where a covered entity or business associate 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.

xvii. Based on the details collected, the university will determine if the security incident resulted in a breach requiring notification. If notification is required, the university will adhere to the policy outlined in Section 5.3, below.

*5.3 **Data Breach Notification***

xviii. If it is determined that a data breach has occurred, the university will perform the following notifications:

5.3.1. **Individual Notice:**

xix. The university will provide individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.

xx. If the university has insufficient or out-of-date contact information for 10 or more individuals, alternate or substitute notification methods will be used.

xxi. Individual notifications will be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach. Notifications will include, to the extent possible:

- a brief description of the breach,
- a description of the types of information that were involved in the breach,
- the steps affected individuals should take to protect themselves from potential harm,
- a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, and
- contact information for the covered entity

5.3.2. **Notification to the Secretary of Health and Human Services**

xxii. In addition to notifying affected individuals, the university will notify the Secretary of breaches of unsecured protected health information. The university will notify the Secretary by visiting the HHS website and filling out and electronically submitting a breach report form.

xxiii. If a breach affects 500 or more individuals, the university will notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals,

the university may elect to notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

5.3.3. **Notification to the Media**

xxiv. If the university experiences a breach affecting more than 500 residents of a State or jurisdiction, the university will, in addition to notifying the affected individuals and the Secretary of HHS, provide notice to prominent media outlets serving the State or jurisdiction.

xxv. This notification can be in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification will be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and will include the same information required for the individual notice.

5.3.4. **Notification by a Business Associate**

xxvi. If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the university following the discovery of the breach. A business associate must provide notice to the university within the timeframe specified in the Business Associate Agreement between the parties.

xxvii. To the extent possible, the business associate will provide the university with the identification of each individual affected by the breach as well as any other available information required to be provided by the university in its notification to affected individuals.

Section 6: Policy Documentation Requirements

6.1 Documentation (164.316(a))

xxviii. The University of Puget Sound will implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. When designing and implementing measures to comply with the HIPAA Security Rule, the following items will influence the security program:

- **The university's size, complexity, and capabilities**
- **The university's technical infrastructure, hardware, and software capabilities**
- **The costs of security measures**
- **The probability and criticality of potential risks to electronic protected health information**

xxix. The HIPAA Security Rule and this policy manual are not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements. The University of Puget Sound may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this policy manual.

6.2 Documentation Maintenance (164.316(b)(1))

xxx. The University of Puget Sound will maintain the policies and procedures implemented to comply with The HIPAA Security Rule in written form. If an action, activity, or assessment is required by HIPAA or this policy to be documented, the university will maintain a written record of the action, activity, or assessment.

xxxi. These written records may be in electronic form (164.316(b)(2)) and will be:

- **Retained for six years from the date of their creation or the date when they last were in effect, whichever is later**
- **Made available to those persons responsible for implementing the procedures to which the documentation pertains**
- **Reviewed periodically, and updated as needed, in response to environmental or operational changes affecting the security of the electronic protected health information**

Section 7: Document Authorization

This document has been reviewed and accepted by the following:

NAME	POSITION	SIGNATURE	DATE

ADDENDUM A Revision History

Name	Date	Changes	Reviewed by Technology Services Yes/No
Ann Wilson	4/27/16	• Revised encryption policy (addendum B) and verification of HIPAA training and confidentiality agreement added	Yes
Ann Wilson	1/4/17	• Revised encryption policy, verification of HIPAA training and confidentiality and student PHI contract	Yes
Ann Wilson	4/26/17	• Moved HIPAA training and confidentiality agreement and student PHI contract into Privacy Policies • Added Appendices A-D to Privacy Policies • Added language from HHS regarding electronic communications (email) with patients • Added explicit language re photographic images as PHI to Privacy Policies and appended Photography Consent form to appendix.	Yes
Ann Wilson	12/13/17	• Revised Privacy and Security portions of the document to include the addition of My Clients Plus™ as the ePHI system used by the OT onsite clinic. • Revised language to include the OT mental health clinic experience that takes place off campus and is therefore not part of the onsite clinics but is covered by the university's HIPAA privacy and security policies.	Yes

		• Revised Encryption Agreement, PHI contract and HIPAA training certification to reflect the addition of My Clients Plus and the inclusion of the OT mental health clinic	
Ann Wilson	5/8/18	• Added description of audit process used in OT onsite clinic. • Added description of the secure use of scanner to scan paper documents into WebPT.	Yes
Ann Wilson	7/15/19	• Reviewed entire document. Corrected minor typographical errors	Yes
Ann Wilson	7/29/2020	• Reviewed entire document.	
Sheryl Zylstra	1/17/21	Edited to reflect OT students using UPS HIPAA compliant Google Drive for documentation purposes this spring semester.	
Amy Kashiwa Amy Snell	12/28/2021	Reviewed entire document	Yes

– Personal Device Encryption

School of Physical Therapy
Encryption of Personal Devices for Access to Electronic Health Records (EHR) Policy
Revised 12/2017; Reviewed 7/2019; 7/2020

All users of WebPT who intend to access WebPT using their personal device must have the device encrypted. The procedure and instructions for encrypting personal devices can be found at http://www.pugetsound.edu/about/offices-services/technology-services/help-support/data-encryption/ **PLEASE READ THIS INFORMATION CAREFULLY BEFORE PROCEEDING WITH THE ENCRYPTION TO AVOID ANY DAMAGE TO PERSONAL DEVICES.**

Members of the university community (students and clinical instructors) whose personal devices cannot be safely encrypted using the procedure above may access WebPT on their personal device through the V Desk. Instructions for setting V Desk up can be found at http://vdesk.pugetsound.edu.

All users of WebPT who intend to access it with a personal device must indicate acknowledgment of the requirement to maintain an encrypted environment at all times. Failure to use some form of encryption may result in revocation of their privileges to access to WebPT.

Acknowledgment and Agreement

I, _____, understand that I am required to access WebPT on an encrypted computer at all times.

Please check the appropriate box(es):

☐ My personal computer has been encrypted via the one of the processes described above.

☐ My iPad has been secured with a pass code or the tablet device I am using has been encrypted.

☐ I have installed V Desk according to the instructions provided and will only access WebPT on my personal device through browsers within V Desk.

☐ I do not plan to access WebPT on my personal device. Instead, I will only access WebPT on a university owned desktop or laptop device that has been encrypted.

I further understand that accessing WebPT on a personal device that is not encrypted is grounds for revocation of my access to WebPT.

_____ _____
Signature Date

Title or Designation (Please check one)

☐ Clinical Instructor
☐ Student Therapist
☐ Office Support Staff
☐ Other (please describe) _____

Revised 12-2023; 01-2025; 08-2025

School of Occupational Therapy
Encryption of Personal Devices for Access to Electronic Health Records (EHR) Policy
Revised 12/2017; Reviewed 7/2019; Revised 1/21

All occupational therapy students using their personal device to document in the onsite clinic must have the device encrypted. The procedure and instructions for encrypting personal devices can be found at:http://www.pugetsound.edu/about/offices-services/technology-services/help-support/data-encryption/

PLEASE READ THIS INFORMATION CAREFULLY BEFORE PROCEEDING WITH THE ENCRYPTION TO AVOID ANY DAMAGE TO PERSONAL DEVICES.

All users with a personal device must indicate acknowledgment of the requirement to maintain an encrypted environment at all times. Failure to use some form of encryption may result in revocation of their privileges to document on a personal device.

Acknowledgment and Agreement

I, _____, understand that I am required to conduct clinic documentation on an encrypted computer at all times.

Please check the appropriate box(es):

□ My personal computer has been encrypted via the one of the processes described above.

□ My iPad has been secured with a pass code or the tablet device I am using has been encrypted.

□ I do not plan to document on my personal device. Instead, I will only document on a university owned desktop or laptop device that has been encrypted.

I understand that documenting client data on a personal device that is not encrypted is considered a HIPAA breach.

_____ _____
Signature Date

Title or Designation (Please check one)

□ Clinical Instructor
□ Student Therapist
□ Office Support Staff
□ Other (please describe) _____

Revised 12-2023; 01-2025; 08-2025