POLICY AND PROCEDURE HANDBOOK

EXPERIMENTAL EDUCATION UNIT

Early Support Program

Updated 7/2024

Table of Contents

Contacts

Early Support Program Coordinator	Laura Crawford
Family Resource Coordinator (FRC)	Betsy McAllister
Fiscal Specialist	Serianna Block
ClinicNote Contact	Lana Fox
Related Service Coordinator	Molly Tellone
EEU School Principal	Chris Matsumoto
Program Support Specialist	Babie Jahmid

CLINICNOTE TRAINING

Create an account using the links below:

- **Supervisors/Faculty:** https://clinicnote.thinkific.com/enroll/1043218?price_id=1157170
- **Billing Personnel:** https://clinicnote.thinkific.com/enroll/2099394?price_id=2842224

1. In the provided fields, enter your first and last name
2. Enter your email address into the provided field
3. Create a password in the provided field
4. Click the “Sign Up” button

EEU DIRECT SERVICE PROCESS

Part One:

1) IFSP meeting is held and services are determined.
2) If direct services are recommended, **FRC** gives families the following*:
    a. SOPAF
    b. Haring Center billing agreement with attached notice of privacy practices, non-discrimination policy, and financial assistance policy
    c. Physician Referral Form
3) **Therapists** schedule first visits at IFSP meeting or if not able, copy **FRC** on first emails to schedule visits.
4) **FRC** collects paperwork along with front/back copy of insurance card
5) Once **FRC** has the following 4 documents, she gives them to the **early support director** in **one packet**
    a. Referral from doctor
    b. Copy of insurance card
    c. SOPAF
    d. Haring Center billing agreement
6) **Early support director** inputs documents into clinicnote and assigns **therapists**
7) If these documents are not collected before services start, we may end up needing to hold billing and retroactively go back to put diagnosis code, CPT code, etc. in to the system so we can bill for those dates.
    a. If something happens where insurance is not approved, that is okay because the family attempted to participate in the cost.
    b. If a family ends up deciding to pay the family fee, then we would go back and charge the monthly family fee.
8) **Program support specialist** calls insurance companies on behalf of clients in order to check benefits and gain pre-authorizations for evaluations and treatment (this happens for some clients initially and may need to call again every 6 months-1 year)
    a. **Program support specialist** lets insurance company know if secondary or tertiary insurance is involved
9) Families agree in the billing agreement to let the FRC know of any changes to insurance (addition or subtraction of secondary or tertiary)
    a. **FRC** should notify **early support director** of any changes as soon as she finds out if there is a change to insurance
10) **Therapists** schedule home visits on the ITP Individual Service calendar (be sure to only use initials)
11) **Therapists** submit notes in clinicnote by end of day Thursday for the week prior. Notes should be submitted directly to create claim if billable and to saved if non-billable.
12) **Early Support Director** checks monthly that all notes have been written, and billable sessions have been submitted to claims
13) **Front Desk** makes sure to forward all paper EOBs and checks to **Fiscal**
14) **Fiscal** opens billing module in clinicnote weekly on Fridays
    a. Looks at “ready” claims, goes through each claim and checks that codes and units look accurate (no more than 4 units/session if 60 minutes).
    b. Electronically submits any “ready” claims available

c. Looks at "submitted" claims, monitors based on information on average length of time it takes to get payment and may need to call insurance companies if it is taking longer than average.
d. Looks at "accepted" claims, checks ERAs and paper EOBs and updates contracted rate, insurance reimbursed, and patient responsibility
    i. Making sure to adjust invoices accordingly for patients on financial assistance

15) **Fiscal** logs on to ability network weekly on Fridays
    a. Checks claims for errors, corrects errors, and then makes sure claims go through
    b. Checks claim status to look for any rejected claims
        i. Looks at paper EOBs if needed to resolve rejected claims or uses information inputted from ERA to resolve rejected claims. Make sure to follow steps on clinicnote billing module.
16) **Fiscal** creates invoices and sends statement to family at the end of each month
    a. As payment comes in, Fiscal adjusts invoices, re-sends invoices monthly as needed
17) **Fiscal** meets monthly with early support director, school principal, and related service coordinator to make everyone aware of any billing/client issues and any updates

PAYMENT AND FINANCIAL ASSISTANCE PROCESS

1) Families are made aware by the FRC at the IFSP if services they are receiving are subject to Family Cost Participation per ESIT's System of Payments and Fees

2) Options for Family Cost Participation are as follows:
    a. Public Health Care Coverage/Insurance (Apple Health for Kids/Medicaid)
    b. Private Health Care Coverage/Insurance
    c. Family Fee/Sliding Scale

3) All families are made aware of the Financial Assistance Policy by the FRC at the IFSP

4) Families are given a copy of the Financial Assistance Policy and application if they are interested

5) Families fill out the Financial Assistance Application and if they need help, they work with the FRC to fill it out

6) Financial Assistance Applications are turned in to the FRC, Haring Center Assistant Director determines if they qualify within 14 days based on the Financial Assistance Care Review Process and uses the Financial Assistance Care Review Sheet

7) Haring Center Assistant Director informs the **Fiscal** of families that qualify for a reduction, and if so what percent or the maximum monthly amount

8) **Fiscal** Specialist adjusts all patient bills according to qualification level

*Please note, it is required that documents be translated if requested. The following documents should be translated:

1) SOPAF
2) Notice of Privacy Practices
3) Haring Center billing agreement
4) IFSP (*If any confidential patient data is translated, a translated release form must be signed)
5) Patient bills
6) Financial Assistance Policy
7) Financial Assistance Application
8) Financial Assistance award/denial letters
9) *If a non-commercial interpreter is engaged, please have the patient sign a translated release

DOCUMENTATION GUIDE

DIRECT NOTES (items in grey should be auto-populated):

<table>
<tr><td>Patient name</td><td colspan="2">Place of service
Home
Independent Clinic (EEU)
School (Daycare)
Other place of service (Community)
Telehealth provided in patient’s home
Telehealth services other than in patient’s home</td></tr>
<tr><td colspan="3">DOB</td></tr>
<tr><td colspan="3">Allergies</td></tr>
<tr><td colspan="3">Referring Physician</td></tr>
<tr><td>Date (of service)</td><td>Start Time</td><td>End Time</td></tr>
<tr><td colspan="3">Diagnosis Code</td></tr>
<tr><td colspan="3">CPT Code(s): If more than one diagnosis, enter CPT code(s) under diagnosis that corresponds to your discipline. *If your session is non-billable, do not put a CPT code (i.e. if child was asleep, no diagnosis, etc.)</td></tr>
<tr><td colspan="3">Goals: Click on a goal to expand it to find outcomes and unselect the box that say “show on note” it if it is NOT a goal you worked on during your session</td></tr>
<tr><td colspan="3">Previous Plan: Will auto-populate based on last note
If first session, you can note that there was no previous plan</td></tr>
<tr><td colspan="3">Subjective
In this section you should put “subjective” info that the patient provides to you during the session. In our case, this will most likely be a family update on how things have been going.</td></tr>
<tr><td colspan="3">Objective
Select “combine objective comments” if you want to combine all goals into one comment field, otherwise you can comment separately. You do not need to fill in the “value boxes.”
In this section you should write your observations of how the child is doing on their goals.</td></tr>
<tr><td colspan="3">Assessment
Select all goals you would like to comment on
You can also just combine assessment comments if you want
In this section you should write your assessment of how the child is doing on their goals (I.e. are they improving, or what factors are contributing to progress/lack of progress)</td></tr>
<tr><td colspan="3">Plan for next session
This does not have to be long, unless you have something special to add, you can just say “continue plan of care,” “assess progress at next session” or a specific plan you have to target something.</td></tr>
<tr><td colspan="3">Previous home based therapy tasks</td></tr>
<tr><td colspan="3">Home based therapy tasks
You can copy/paste from previous if you want and edit as needed or add new</td></tr>
<tr><td colspan="3">Additional comments: Any other relevant information.*If this is a makeup session please note by writing “This is a make-up session for session missed on XX/XX/XXXX.” **Please write “DO NOT BILL” in this section if it is a non-billable session and write why (i.e. child was asleep, etc.).</td></tr>
<tr><td colspan="3">Signature: you will electronically sign here</td></tr>
<tr><td colspan="3">Click “save and create/update claim” unless non-billable, then just click “save note”</td></tr>
</table>

CANCELED SESSION (items in grey should be auto-populated):

Patient name	**Place of service** (where you were planning) • Home • Independent Clinic (EEU) • School (Daycare) • Other place of service (Community) • Telehealth provided in patient's home • Telehealth services other than in patient's home	
DOB		
Allergies		
Referring Physician		
Date (of canceled service)	**Start Time** (planned)	**End Time** (planned)
Diagnosis Code		
CPT Code(s): Leave BLANK		
Goals: Don't need to change		
Previous Plan: *Will auto-populate based on last note*		
Subjective: Leave BLANK		
Objective: Leave BLANK		
Assessment: Leave BLANK		
Plan for next session: If you have already rescheduled, note what date you have planned, otherwise leave blank		
Previous home based therapy tasks		
Home based therapy tasks: Leave BLANK		
Additional comments: In this section you should put "CANCELED SESSION DUE TO _____ (FILL IN REASON SESSION WAS CANCELED)" also please write "DO NOT BILL"		
Signature: you should electronically sign here		
Click "save note"		

CONSULTATION NOTES (items in grey should be auto-populated):

<table>
<tr><td>Patient name</td><td colspan="2">Place of service (choose where the majority of consultation services were provided for the month)
Home
Independent Clinic (EEU)
School (Daycare)
Other place of service (Community)
Telehealth provided in patient’s home
Telehealth services other than in patient’s home</td></tr>
<tr><td colspan="3">DOB</td></tr>
<tr><td colspan="3">Allergies</td></tr>
<tr><td colspan="3">Referring Physician</td></tr>
<tr><td>Date: If you are documenting a specific date when you had a lengthy consultation you can indicate that, otherwise just select the last day of the month</td><td>Start Time: Unless you are documenting a single consultation session, you should just choose a start and end time that correspond with the total amount of time you spent consulting during the month.</td><td>End Time: You should also include any minutes of consultation that were not delivered in the month to account for all minutes written on the IFSP.</td></tr>
<tr><td colspan="3">Diagnosis Code</td></tr>
<tr><td colspan="3">CPT Code(s): leave BLANK</td></tr>
<tr><td colspan="3">Goals: Click on a goal to expand it to find outcomes and unselect the box that say “show on note” it if it is NOT a goal you consulted on</td></tr>
<tr><td colspan="3">Previous Plan
Will auto-populate based on last note
If first session, you can note that there was no previous plan</td></tr>
<tr><td colspan="3">Subjective
In this section you should put “subjective” info that the patient provides to you during the consultation. In our case, this will most likely be a family update on how things have been going. If you are documenting multiple consultations within the month, please include date, modality, and length of time. Since this is a consultation, you may be summarizing for the whole month. Please also include any minutes not delivered and the reason why.</td></tr>
<tr><td colspan="3">Objective
Leave BLANK unless you have direct observations of the child to report.</td></tr>
<tr><td colspan="3">Assessment
Leave BLANK unless you have a specific comment on assessment outside of what the parent has reported.</td></tr>
<tr><td colspan="3">Plan for next session
This does not have to be long, unless you have something special to add, you can just say “continue plan of care,” “assess progress at next session” or a specific plan you have to target something.</td></tr>
<tr><td colspan="3">Previous home based therapy tasks</td></tr>
<tr><td colspan="3">Home based therapy tasks
You can copy/paste from previous if you want and edit as needed or add new</td></tr>
<tr><td colspan="3">Additional comments: Please write “DO NOT BILL” and any other relevant information.</td></tr>
<tr><td colspan="3">Signature: you should electronically sign here</td></tr>
<tr><td colspan="3">Click “save note”</td></tr>
</table>

DOCUMENTATION FAQ

1. **The previous plan and previous home-based therapy tasks will transfer over from the last person's note, regardless of discipline, is there a way to change that?**
    a. Not at the moment. You can delete/edit the previous plan but not the previous home based therapy tasks. They are working on an update rolling out at the end of July that will hopefully fix this issue.
2. **If I want to come back to a note, how to I get it to show up in my to-do list?**
    a. Do not sign the note if you want to come back to it. Once you sign it, if you save it, it will go to their saved notes.
3. **What if I am supposed to be billing, but the dx code is not listed?**
    a. Please send an email to Laura to let her know that the dx code is not listed (this may also apply if you think a dx code might be missing). In additional comments please write "will use CPT code XXXXX and designate units when diagnosis code is inputted"
4. **Should I write a note for a "canceled session" if we never actually scheduled the session (family was busy, on vacation, had difficulty scheduling, etc.)**
    a. Yes – account for all of your minutes by writing notes even if those visits were never actually scheduled. Use the "cancelled session" format when needed.
5. **If I go over my time for a billable session, should I bill for the whole session, or just the minutes on the IFSP?**
    a. Only bill for the amount of time that is on the IFSP.
6. **What if the child is asleep during the direct service session?**
    a. Fill out a session note but do not bill
    b. If child is sleeping regularly during your session, you may want to consider switching the time
7. **Are we able to use two (or more) different codes in a session (half as speech and half on feeding)?**
    a. For timed codes, yes no problem
    b. For un-timed codes, just use the code for whichever you spent the majority of your session
    c. Less than 15 minutes is not a session for un-timed codes
8. **Can you carry over other discipline's activities/strategies during a session?**
    a. You cannot bill another discipline's code
    b. If the family needs direct assistance with another discipline, they should be receiving that service in addition to your own
9. **Can you do direct service during playgroup?**
    a. Yes, you must have the family fill out "consent to treat in a group setting"
10. **Are we allowed to co-treat?**
    a. There are no specific codes for co-treating
    b. We can co-treat with our own providers occasionally, but only one person can bill, the other provider should write "do not bill"
    c. The program support specialist can check insurance and see if codes would be accepted during a co-treat session with an outside provider
    d. You should not schedule a visit at the same time as another outside provider unless we have confirmed that it will be approved by insurance
    e. If an outside provider is involved, we are going to need to get the CPT code they are using before we can check insurance

f. Encourage the family to also check their own insurance

11. **Can we start individual sessions before billing (for example, a trial session to determine frequency or if it will be a good fit)?**
    a. No
12. **What are the factors used when determining discharge/decreasing frequency?**
    a. Provider will monitor progress, assess and interpret data to make determination using professional judgment (As a professional they need to be able to determine the service is not necessary to make age-appropriate progress.)
    b. Tools used: developmental norms, language sample, CBA's, maybe standardized assessments
    c. Services can be tapered off if the provider uses professional judgement to make the case.
13. **What are the policies on inclement weather and make-up sessions**
    a. Make-up visits:
        i. Typically, visits cancelled by providers need to be rescheduled. for example when the provider is sick or on vacation
        ii. Weather cancellations: providers can offer a make-up session but are not required to do so when the visit is cancelled due to extreme weather.
        iii. When the family cancels a visit, we can work with them to schedule a make-up, but we are not required to do so
    b. Compliance timelines:
        i. If cancelled visits result in late timelines (45-day IFSP, 30-day timely services, and 90-day transition conference), the state guidance is that extreme weather is an acceptable reason. The delay should be documented in the ESIT DMS as "Exceptional Family Circumstance" with an explanation of the weather-related cancellation(s).

CPT Codes

OT and PT Codes		
Code	**Description**	**Rate**
97110	**Therapeutic exercises to develop strength and endurance, range of motion, and flexibility (15 minutes)**	**$31.25/unit**
97112	**Neuromuscular re-education of movement, balance, coordination, kinesthetic sense, posture, and/or proprioception for sitting and/or standing activities (15 minutes)**	**$31.25/unit**
97116	**Gait training (includes stair climbing) (15 minutes)**	**$31.25/unit**
97140	**Manual therapy techniques (e.g. connective tissue massage, joint mobilization and manipulation, and manual traction) (15 minutes)**	**$31.25/unit**
97150	Therapeutic procedure(s), group (2 or more individual) (bill per session, NOT UNITS)	$62.50/session
97530	**Therapeutic activities, dynamic activities to improve functional performance, direct (one-on-one) with the patient (15 minutes)**	**$31.25/unit**
97533	Sensory integrative techniques to enhance sensory processing and promote adaptive responses to environmental demands, direct (one-on-one) patient contact (15 minutes)	$31.25/unit
97535	Self-care/home management training (e.g., activities of daily living [ADL] and compensatory training, meal preparation, safety procedures, and instructions in use of assistive technology devices/adaptive equipment), direct one-on-one contact (15 minutes)	$31.25/unit
97542	**Wheelchair management (e.g., assessment, fitting, training) (15 minutes)**	**$31.25/unit**
97760	**Orthotic(s) management and training (including assessment and fitting when not otherwise reported), upper extremity(s), lower extremity(s) and/or trunk (15 minutes)**	**$31.25/unit**
92526	**Treatment of swallowing dysfunction and/or oral function for feeding**	**$125/session**
98960	**Education and training for patient self-management by a qualified, nonphysician health care professional using a standardized curriculum, face-to-face with the individual patient (could include caregiver/family) (30 minutes)*** **	**$62.50/unit (30 min units)**

SLP Codes		
Code	**Description**	**Rate**
92526	**Treatment of swallowing dysfunction and/or oral function for feeding**	**$125/session**
92507	**Treatment of speech, language, voice, communication, and/or auditory processing disorder, individual**	**$125/session**
92508	group, two or more individuals	$62.50/session
98960	**Education and training for patient self-management by a qualified, nonphysician health care professional using a standardized curriculum, face-to-face with the individual patient (could include caregiver/family) (30 minutes)*** **	**$62.50/unit (30 min units)**
92606	Therapeutic service(s) for the use of non-speech generating augmentative and alternative communication device, including programming and modification	$125/session
92609	Therapeutic services for the use of speech-generating device, including programming and modification	$125/session
V5336	Repair/Modification of AAC device (excluding adaptive hearing aid)	$125/session

*1 unit = 8-15 minutes

**except when using 98960: 1 unit = 15-30 minutes

***Please see section on using the HELP at Home when billing this code

PARENT COACHING MODEL AND GENERAL GUIDELINES

- Goals of Parent Coaching:
    - Help parents recognize what they are **already doing** that promotes their child's learning
    - Assist parents in creating ongoing learning opportunities for the child when the home visitor is not present

- Caregivers and service providers partner together to work on skills that promote the child's participation in activities across family and community settings.

- During the visit, the family will identify routines and other times in which they would like support.

- The service provider will help by collaborating on strategies to work on the identified skills, developing a plan, and modeling.

- Caregivers are encouraged to participate by trying out strategies during the session and by receiving support, feedback, and suggestions for working on the new skill from the service provider.

- At the end of the session, caregivers and service providers mutually agree on activities and skills to practice in between visits.

SAFETY

Before the home visit	During the home visit
• Notify co-workers (use the home visit calendar, include address) • Review in take form or talk to other team members for any possible concerns about violence • Bring your cell phone • Park your car in a place that enables you to leave quickly • Wear your ID badge	• Be aware of exit • Sit near an exit, within view of hall, bedrooms • Use non-threatening body language • Respect client's home • Be aware of pets
Other safety tips	
• Back your car into a parking spot • Bring dog biscuits to calm aggressive/excited dogs • Ensure car has gas, is in working condition • Refrain from sharing personal details • Trust your intuition • Debrief with a co-worker	

MILEAGE AND TOLL REIMBURSEMENT

1. Submit a TREQ (request) for mileage reimbursement from now on. If any staff member currently do not have access to TREQ, kindly send an email to edfiscal@uw.edu. Our team will promptly set them up with access and provide the necessary training materials
2. Along with the TREQ, submit the mileage form found at: https://education.uw.edu/my-coe/facstaff/fiscal-office/forms
3. Please see the step by step tutorial in the following program meeting recording: August Program Meeting 2023

Please direct all questions to hcfiscal@uw.edu

HIPAA TRAINING AND GUIDELINES

Required Training:

- All Haring Center employees working in ITP must complete the Compliance Learning Portal (CLP) at: https://uwmedicinecompliance.uw.edu/
- All Haring Center employees working in ITP must also read and sign the Haring Center ITP Employee Privacy Confidentiality and Security Agreement

Use of Email and Texting:

Sending patient information via email within ITP teams

You may send patient information via email within ITP teams as long as the following requirements are met

1. The email is sent within UW (@u.washington.edu, @uw.edu) between ITP team members
2. The email transmission is secure by using Outlook
3. The email contains the minimum amount of patient information necessary to meet the recipient's needs.

Using Outlook/UW Exchange/UW Office 365

All employees working in ITP are required to send and receive their UW email on UW Exchange (also known as UW Office 365), which is the only UW Medicine-approved email service available. This policy is in place to ensure the proper handling of HIPAA-protected information that you may send and receive. Please note employees working in ITP are prohibited from forwarding their UW email to UW Gmail or any other personal account.

Please contact EEU tech (eeutech@uw.edu) if you need help configuring your email to outlook.

The following language should be included under your signature on any email sent to a patient:

"The above email may contain patient identifiable or confidential information. Because email is not secure, please be aware of associated risks of email transmission. If you are a patient, communicating to a Haring Center Provider via email implies your agreement to email communication per the billing agreement.

The information is intended for the individual named above. If you are not the intended recipient, any disclosure, copying, distribution or use of the contents of this information is prohibited. Please notify the sender by reply email, and then destroy all copies of the message and any attachments."

What to do if an email containing patient information is sent to the wrong recipient:

If you are the sender, notify the school principal immediately. If you are the recipient, immediately reply to the sender notifying them of the error, delete the email and notify the school principal.

Emailing and texting patients:

You may email or text a patient if they have signed the billing agreement section agreeing to receive email and text messages.

*Please make sure all emails are deleted permanently unless the email needs to be retained in the patient file (in which case it should be printed and placed in the patient file)

In addition when texting, you must add encryption to your personal device by using the following steps:

- use of WhatsApp (you and the patient)
- check to ensure data protection on your phone (from UWtech: The first thing to do is make sure that you have a passcode turned on to unlock your phone. I recommend a six digit passcode to

increase security. Once that has been established you can go to Settings -> Passcode and scroll down to the bottom and make sure it says “Data Protection is enabled”)

Saving Files with Patient Data on Computers

- ANY document containing patient data must be stored locally on your computer (i.e. in your documents folder and NOT in the shared drive).
- Only within early support teams- you may also use OneDrive to share documents or use outlook to email to each other
    - If you need to share documents with anyone outside of your ITP team, aside from the patient who has signed the billing agreement, you must contact administration to have that person trained in HIPAA and sign the Haring Center ITP Employee Privacy Confidentiality and Security Agreement

HIPAA Guidelines

HIPAA is a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. Developed by the Department of Health and Human Services, these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this new rule. HIPAA took effect on April 14, 2003

Patient Rights

- To get an electronic or paper copy of their medical record
- To ask to correct their medical record
- To request confidential communications
- To ask their provider to limit what they use and share
- To get a list of those with whom their provider has shared information
- To get a copy of the privacy notice
- To choose someone to act for them (medical power of attorney or legal guardian)
- To file a complaint if they feel their rights are violated

Patient Choices

- In these cases, patients have both the right and choice to tell their provider to:
    - Share information with their family, close friends, or others involved in their care
    - Share information in a disaster relief situation
    - Include their information in a hospital director
- In these cases, providers may *never* share patient information unless given written permission:
    - Marketing purposes
    - Sale of patient information
    - Most sharing of psychotherapy notes
- In the case of fundraising:
    - The provider may contact the patient for fundraising efforts, but the patient may tell the provider to not contact them again

Health Information and Disclosures

Providers can use or share patient health information in the following ways:

- Treatment: use patient health information and share it with other professionals who are treating
- To run the organization: use and share patient health information to run the practice, improve patient care, and contact patients when necessary
- Bill for services: use and share patient information to bill and get payment from health plans or other entities

Providers are allowed or required to share patient information in other ways:

- To help with public health and safety issues in certain situations
- To do research
- To comply with the law
- To respond to organ and tissue donation requests
- To work with a medical examiner or funeral director
- To address workers' compensation, law enforcement, and other government requests
- To respond to lawsuits and legal actions

Provider Responsibilities

- We are required by law to maintain the privacy and security of patient protected health information (PHI)
    - Name
    - Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
    - All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
    - Telephone numbers
    - Fax number
    - Email address
    - Social Security Number
    - Medical record number
    - Health plan beneficiary number
    - Account number
    - Certificate or license number
    - Any vehicle or other device serial number
    - Web URL
    - Internet Protocol (IP) Address
    - Finger or voice print
    - Photographic image - Photographic images are not limited to images of the face.
    - Any other characteristic that could uniquely identify the individual
- We will promptly let the patient know if a breach occurs that may have compromised the privacy or security of patient information
- We must follow the duties and privacy practices described in the privacy practices notice and give patients a copy
- We will not use or share patient information other than as described above unless the patient tells us we can in writing. If the patient tells us we can, the patient may change their mind at any time.

Early Support Security Officer Roles and Responsibilities

Name of Security Officer: Molly Tellone

Roles and Responsibilities

- Develop and maintain the "Haring Center Security Policies and Procedures" with input from the EEU director, early support lead, building manager, UW Healthcare Compliance, and UW IT services
- Develop and maintain the "Haring Center Disaster Recovery Policy" with input from the EEU director, early support lead, building manager, UW Healthcare Compliance, and UW IT services
- Review and update the "Haring Center Security Policies and Procedures" annually and as needed
- Review and verify that workforce members have completed HIPAA training and reviewed security procedures annually, maintain a comprehensive record of all personnel who have completed training
- Maintain a list of personnel who can have access to the PHI and communicate with EEU director and UW IT services to ensure workforce members' access and privileges are minimum necessary (i.e. need to know) based on their roles
- Develop and maintain "Offboarding Checklist" for employees exiting the early support program
- Develop and maintain "Authorization form and the procedure for releasing PHI"
- Develop consent forms related to privacy policies and procedures
- Develop new security procedures as needed when new systems are introduced or current systems require a change

- Receive reports of potential breaches of PHI from Haring Center workforce members
- Work with EEU director to report received potential breach notifications to the UW CRS Privacy and Compliance Program Manager and work with CRS Privacy and Compliance Program Manager to investigate the event and gather information relevant to the incident
- Assist in remediating identified issues related to potential breaches of PHI as needed

- Attend Haring Center Early support meetings as needed and present on topics related to security policies and procedures
- Attend bi-monthly Health Care Component Group meetings run by UW Healthcare Compliance, communicate necessary information from these meetings to Haring Center staff, and update policies and procedures as needed
- Send at least quarterly email policy reminders to all Haring Center early support staff

- Complete annual "Security Risk Assessment (SRA)" with input from the EEU director, early support lead, building manager, UW Healthcare Compliance, and UW IT services
- Review results of the SRA with UW Healthcare Compliance manager to develop corrective action plans
- Send written and verbal communication around the corrective action plans with the EEU director, early support lead, and UW IT services

- Answer questions and act as a resource for Haring Center early support staff and students when they have security policy questions

UW Healthcare Components Compliance Group Breach Documentation And Notification Process

Table of Content

HIPAA and non-HIPAA health information breach Notification Rule

The Policy:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the rule which compromises the security or privacy of protected health information. The Health Insurance Portability and Accountability Act (HIPAA) and in accordance with all State and Federal laws and regulations, requires HIPAA and non-HIPAA health care entities and their business associates to provide notification following a breach of unsecured protected health information.

1. Purpose

The purpose of this policy is to establish the following:

- The process UW Healthcare Components Compliance Group (HCCG) follows to report potential breaches of protected health information (PHI) to UW Compliance and Risk Services (CRS) and refer potential breaches of non-PHI University Personal Data to the appropriate department.
- UW CRS obligation to ensure notification to patients and other parties of a breach of PHI.
- The parties must be notified by specified timelines.
- Required content of notifications.
- Responsibility for implementation.

2. Process

UW (HCCG) workforce members shall report potential breaches of PHI to their Privacy Liaison and the Liaison report these breaches to the UW CRS Privacy and Compliance Program Manager. The CRS Privacy and Compliance Program Manager will work with each unit privacy liaison to ensure that the event has been fully investigated and they had collected all the information relevant to this incident. The CRS Privacy and Compliance Program Manager shall review all relevant facts of a reported event to determine if a breach of PHI has occurred, which may include a formal risk assessment based on required factors to determine the probability that the PHI has been compromised. If a breach is confirmed, the CRS Privacy and Compliance Program Manager will ensure that written notification is provided to appropriate parties. The HCCG unit in which the

potential breach occurs shall cooperate with the investigation, assist in remediating identified issues and may be responsible for funding the response and notification of affected patients.

3. Assessment of Potential Breach Involving Protected Health Information

A. UW CRS Privacy and Compliance reviews all relevant facts of the reported event and determines if the acquisition, access, use or disclosure of PHI:
   1. Was not for treatment, payment, or healthcare operations;
   2. Was not authorized by the patient; and
   3. Was not otherwise allowed by law.

B. UW CRS Privacy and Compliance determines if the circumstances meet any of the following breach notification exceptions:
   1. An unintentional acquisition, access or use of PHI by a workforce member or business associate who is acting in good faith within the scope of their authority (providing it does not result in further impermissible use or disclosure);
   2. An inadvertent disclosure of UW HCCG PHI between two persons who are both authorized to access UW HCCG PHI, providing the information received as a result of such disclosure is not further impermissibly used or disclosed; or
   3. A disclosure of PHI to an unauthorized person, who UW HCCG believes, in good faith, would not reasonably have been able to retain such information.

C. UW CRS Privacy and Compliance may still demonstrate that there is a low probability that the PHI has been compromised by conducting a formal risk assessment based on a minimum of the following factors:
   1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   2. The unauthorized person who used the PHI or to whom the disclosure was made; Whether the PHI was actually acquired or viewed; and
   3. The extent to which the risk to the PHI has been mitigated.

D. If none of the exclusion criteria apply and a low probability of compromise to the PHI cannot be demonstrated, a breach of PHI is confirmed, and UW CRS Privacy and Compliance ensures completion of the notification process.

4. Parties Required to be Notified if breach is determined

A. The patient(s).
B. The Secretary of the Department of Health and Human Services (DHHS).
C. The Washington State Attorney General (when a security breach involves more than 500 Washington state residents).
D. The Federal Trade Commission (FTC) for non-HIPAA health care entities if the breach involves the information of 500 or more people.
E. The local media (when a privacy breach involves more than 500 residents of any given state or jurisdiction).

5. Notification Timelines

In general, notifications are made as soon as possible, without unreasonable delay and in no case later than 60 calendar days after the breach discovery date.

Exceptions:

- Notification may be delayed if it would impede a criminal investigation or cause damage to national security.
- If a breach involves less than 500 patients, the timeframe for notification to DHHS is within 60 days of the end of the calendar year in which the breach occurred.

6. Required Elements of Patient Notifications

A. Written Notifications

1. Must be sent by UW CRS Privacy and Compliance and signed by the UW CRS Privacy Officer or designee.
2. Must be sent by first-class mail to the patient's last known address (or to the patient's personal representative if the patient is deceased and UW CRS Privacy and Compliance has the personal representative's address). If specified as a preference by the patient, the notification may be sent by email.
3. Must contain the following elements:

- A brief description of what happened, including the breach discovery date and the actual date of the incident, if known;
- A specific description of the unsecured PHI that was involved in the breach (such as full name, Social Security number, date of birth, home address, account number or disability code);
- The steps patients should take to protect themselves from potential harm resulting from the breach;
- A brief description of what UW CRS Privacy and Compliance is doing to investigate the breach, mitigate losses and help prevent further breaches; and
- Instructions for obtaining further information, making inquiries and obtaining assistance (including toll-free telephone number, email address, website or postal address).

B. Alternatives to Written Notification

1. If there is insufficient or out-of-date contact information that precludes direct written notification to 10 or more patients, UW CRS Privacy and Compliance will provide substitute notice. Substitute notice will include a toll-free phone number for obtaining additional information about the breach and may be in one of the following forms:
   - A conspicuous posting for 90 days on the UW HCCG specific unit website;
   - A notice in appropriate print or broadcast media that serve geographic areas
   - where affected patients likely reside;
   - An alternative form of written notice, such as by email or by telephone.
2. If imminent misuse of unsecured PHI is suspected, notification may be by telephone or other means.

7. Documentation Requirements

Written documentation must be maintained to demonstrate completion of the following actions:

- Breach risk assessment; and
- Notification to required parties, including copies of letters

8. Responsibility for Implementation

A. UW CRS Privacy and Compliance Program Manager assesses whether an incident constitutes a breach as defined by the Health Insurance Portability and Accountability Act, makes the relevant recommendation to the UW Privacy Officer for healthcare information.
B. UW CRS Privacy and Compliance Program Manager ensures the required notifications are made and maintains all documentation.
C. The HCCG unit in which the breach occurred may be required to pay for the cost of notifying patients.

9. Breaches Involving Personal Data (non-PHI)

A. Unforeseen events, incidents, and potential or confirmed data breaches of Personal Data that does not constitute PHI must be reported to the department responsible for managing such incidents in accordance with University or entity policy.
B. Communications to persons, other than patients or human subjects, about breaches involving University Personal Data will be made as directed by the University Privacy Officer.

REGULATORY/LEGISLATION/REFERENCES

- Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. §164, Subpart D.
- Privacy of Individually Identifiable Health Information, 45 C.F.R. §164, Subpart E.
- Revised Code of Washington (RCW) 19.255 Personal Information – Notice of Security Breaches.
- RCW 19.86.090 Civil action for damages —Treble damages authorized — Action by governmental entities.
- RCW 42.56.590 Personal information — Notice of security breaches.
- FTC's Health Breach Notification Rule, 16 C.F.R. Part 318 ("the Rule").

PROCEDURE ADDENDUM(s) REFERENCES/LINKS

- UW Medicine Compliance Glossary.
- UW Administrative Policy Statement 2.5 Information Security and Privacy Incident Reporting and management Policy.

Approvals

/s/ Jane Yung 9/1/2022

Jane Yung Date
Executive Compliance and Risk
Officer University of Washington

HARING CENTER EARLY SUPPORT OFFBOARDING CHECKLIST

NAME: _____ LAST DAY: _____

Transition

☐Submit letter of resignation
☐Work with supervisor on notification of coworkers
☐Work with supervisor on notification of families

Turn in technology and any other University property

☐Keys (door, file cabinets)
☐Husky Card
☐Parking Permit
☐EEU Badge
☐iPad
☐Laptop

File Management

☐Provide supervisor with voice mail access code
☐Update your voice mail message to advise callers of your status and a number to call for assistance.
☐Identify files stored on your computer, onedrive, or paper files that are of use to others and upload them to teams
☐Upload any client files to the archived record dropbox

Email Management

☐Either set up an auto-reply email message to let others know of your status or forward your account to another employee. Standard Message should include:

- Your Separation Date
- Who to Contact for assistance and their phone number and email address

---

ADMINISTRATION USE ONLY

☐Unsubscribe from email lists
☐Remove access from teams
☐Remove access from EMR system
☐Contact UW Contracting to remove from insurance contracts

Employee Signature: _____ Date:_____

Supervisor Signature:_____ Date:_____

SECURITY POLICIES AND PROCEDURES

Information Technology Systems summary

Our File Servers/Systems

We utilize UW Office 365 SharePoint/MS Teams environment to house our files. (Insert Link Here)

We utilize Clinicnote, Inc as our EMR and billing system. ClinicNote is a HIPAA compliant, secure, web-based platform that maintains client files, including demographic and personal information, client session notes, reports, and billing records. ClinicNote will keep client files within a secure, cloud-based platform for the duration of our subscription. In the event that we terminate our subscription with ClinicNote, the ClinicNote team will retrieve all client files, save in a zip folder, and return to us electronically, per the signed contract and end of term service agreement.

Our Domain Controllers

We use a Delegated OU of the UW's central AD servers.

Our Public-Facing Website

https://eeuschool.org/?page_id=55 - Managed by the College of Education IT's Web Team

Due Care Strategy

Security Philosophy

The security posture of the UW Haring Center Early Support Program is informed by an overall philosophy that recognizes the need for defense in depth; multiple layers of defense all contributing to the protection of critical information.

- **Least Privilege**. The **SharePoint/MS Teams** environment allows folder- and file-level control of access permission. User access is granted on a per user basis and membership is audited at the end of each academic year. By granting permission to each user only to resources necessary for their job duties, we limit the scope of damage that can be done by unauthorized access.
- **Defense in Depth.** This simply means having several layers of defense, e.g.
    - If the hacker gains control of a UW computer to subvert this, they need login credentials specific to our domain and SharePoint Sites.
    - If they try to use deceptive software to obtain these, our email and virus filters will likely detect and avert this.
    - If they discover such credentials, they may not work, as we routinely deactivate credentials upon employee separation and/or prolonged disuse.

- Even if they obtain currently working credentials, they will find their access limited to that required for the job duties of the corresponding employee.
- Even if they obtain credentials with superior access, this will likely be discovered during our routine internal audits of roles and access.

Information Risk

Compliance
As a health care provider, compliance with HIPAA is critical to our center. The Microsoft Office 365 environment uses SSL/TLS connections for data that is in transit from the client to the server. All SSL connections are established using 2048-bit keys. Data at rest uses Advanced Encryption Standard (AES) with 256-bit keys and is Federal Information Processing Standard (FIPS) 140-2 compliant.

https://learn.microsoft.com/en-us/purview/data-encryption-in-odb-and-spo

Operational
Our services are predominantly non-technical, such that most of our computing consists of basic word processing, note taking, and emailing performed locally on our respective computers. One Drive sync client is configured to backup local computer's desktop and documents folders.

Reputational
Again, as a health care provider, the security of PHI is paramount, and breaches of privacy potentially costly due to fines, though more likely are minor mishaps leading to embarrassment of the center and/or UW when the incident is reported, and a corresponding loss of trust by our clients.

Existing controls / Existing Security Architecture

The SharePoint Site collection we utilize has external sharing turned off. Persons without authorized @uw.edu credentials will not be able to access any parts of the SharePoint site collection.

We use Active Directory and a Windows Domain to manage computer configuration and user credentials and assign permissions to users with principle of Least Privilege in mind.

We use Windows Defender or Sophos anti-virus on all computers.

We utilize BitLocker to enable disk encryption on Windows devices.

We deactivate employee credentials upon separation.

We periodically review user access for appropriateness.

We periodically review our information systems for how security settings can be implemented to safeguard ePHI.

Activity on systems which create or use ePHI are recorded are examined through procedural mechanisms *need to include complete inventory of systems that record activity and how it is examined.

We periodically review our information systems to identify and mitigate technical vulnerabilities.

Appendices

Detailed Controls

Data Retention and Destruction
Digitized client files are organized by client date of birth to facilitate records retention in compliance with University policy, and stored on our file server for up to a year after seeing the client, and are migrated to our archival SharePoint document library thereafter until the applicable retention period has elapsed.

Backups
Data is stored in Microsoft's Azure blob storage and is replicated across regional datacenter to ensure redundancy. Items that are deleted follow a deletion flow. This consists of a first and second stage recycle bin. Data is kept across these two recycle bins for a total of 93 days before permanent deletion.

Disaster Recovery Plan
See our Waitlist Information System Contingency Plan and Disaster Recovery Plan.

Remote Access
Recommended best practice to utilize the Husky-On Net VPN for all internet traffic when working from off campus.

Authentication
Authentication is performed via UW Delegated OU structure and UW Office 365 authentication portal. Duo 2FA is also in place.

Intrusion Detection, Logs, and Alerts
The SharePoint infrastructure is monitored by UW-IT's Productivity Platform group

Physical Locations of Storage/Equipment/People

Our servers are in Microsoft's Data Centers. Our offices in the Haring Center building are behind locked doors. Our employees keep physical PHI files in locking drawers, and lock their computers when not in use. PHI is not stored locally on employee computers, all files are stored on the SharePoint infrastructure. Our treatment rooms contain only cameras and a laptop that is disconnected from our computing domain and used only for supervised camera access (an employee must type in a password before each use).

Uses and Disclosures of PHI Requiring a Patient's Opportunity to Agree or Disagree

A. Law Enforcement: Photographing Patients and Obtaining Evidence

When a patient arrives from an accident or incident in which law enforcement is interested but the patient is not in the custody of law enforcement, law enforcement officials may not photograph the patient, obtain evidence or enter the patient care area unless the healthcare entity obtains the patient's permission.

If the patient is not able to provide permission, a manager/administrator may exercise professional judgment as appropriate to allow law enforcement to photograph the patient and/or obtain evidence.

B. Family, Friends and Other Designated Individuals Involved in the Care or Payment of Care

A. Use or disclosure requirements.

Workforce members may use or disclose PHI to assist in the patient's care or to notify a family member, personal representative or other person responsible for the care of the patient only in one of the following situations:

- When the patient agrees to the use or disclosure.
- When the patient is given an opportunity to agree or object and does not object to the use or disclosure.
- When the patient is a minor and the disclosure complies with section 6 below.
- When the patient is not present or is incapacitated, or the circumstances are emergent, and the workforce member has determined, based upon professional judgment or good medical practice, that the use or disclosure is in the best interest of the patient.
- When the patient is deceased and a personal representative of the deceased patient exercises all of the deceased patient's rights. If there is no personal representative, or upon discharge of the personal representative, a deceased patient's rights may be exercised by persons who would have been authorized to make healthcare decisions for the deceased patient when the patient was living.

Patients may instruct in writing not to make disclosures to the patient's immediate family members (including a patient's state registered domestic partner), a personal representative, or any other individual with whom the patient is known to have a close personal relationship.

B. Minor patients.

Workforce members may disclose PHI to a minor patient's parent, guardian or other person acting in loco parentis who has authority to make decisions for a minor regarding the use, access or disclosure of the minor's PHI, except in the following situations:

When the minor is emancipated, the minor is treated the same as an adult with respect to use and disclosure of the minor's PHI.

When the minor may lawfully consent to a healthcare service without parental consent under Washington State law and the minor does not want information about the service disclosed to a parent, guardian or other person acting in loco parentis, workforce members shall not disclose the visit information or services to a parent or others or bill the services to

the parent's or other's insurance, without the minor's consent (with one exception* noted below)

In Washington State, minors may request that PHI related to the following services not be disclosed to a parent, guardian or other person acting in loco parentis, or billed to that individual's insurance:

STD treatment/testing, to include HIV (if 14 years of age or older);

Uses and Disclosures of PHI Requiring Patient Authorization

a. Birth control services (any age);
b. Abortion services (any age);
c. Prenatal care services (any age);
d. Outpatient or inpatient mental health services* (if 13 years of age or older);
e. Outpatient substance abuse treatment (if 13 years of age or older);
f. Inpatient substance abuse treatment (if 13 years of age or older and the Washington State Department of Social and Health Services determines he or she is a child in need of services).

Exception: Workforce members shall disclose the following information to a minor's parent(s) in order to comply with Washington state reporting requirements for a minor's voluntary admission for inpatient mental health services:

- The minor has been admitted to inpatient treatment;
- The location and telephone number of the facility providing such treatment;
- The name of a professional person on the staff of the facility providing treatment who is designated to discuss the minor's need for inpatient treatment with the parent; *and*
- The medical necessity for admission.

i. When a parent who has the authority to consent for a minor chooses to permit certain healthcare services to be confidential between healthcare professionalsand the minor, the minor may make decisions concerning Haring Center's use and disclosure of the PHI related to the services.

ii. When there is documentation that a court has terminated the parental rights of one or both parents, Haring Center workforce members shall not release records to the parent who has lost parental rights. In the absence of such documentation, both parents are deemed to have equal rights and access.

b. If the parent has the right to access the minor's medical record, Haring Center workforce members may release records to both custodial and non-custodial parents.

c. When a minor's mental health information[5] is disclosed for any purpose, the Haring Center workforce member must document the following in the minor's

medical record:

i. The date of the disclosure;
ii. The circumstances under which the disclosure is made;
iii. The name or names of the persons or agencies to whom such disclosure is made;

I. Uses and Disclosures of PHI Requiring Patient Authorization

A. Information Regarding Mental Health, HIV Testing and Other STDs

Heightened standards of confidentiality are required when using or disclosing PHI pertaining to mental health, HIV testing and other STDs. Other than for TPO purposes, most uses or disclosures of this information require patient authorization.

B. Research

Workforce members may use or disclose PHI for research purposes in accordance with HIPAA, the Common Rule and Washington law.

1. PHI, including the PHI of decedents, may be used or disclosed for research purposes only when one of the five following conditions is met:

    a. With a valid authorization of the patient or the patient's personal representative. In the absence of a personal representative for decedents, authorization may be provided by the individual who had authority to make healthcare decisions on behalf of the deceased patient.

        i. An authorization is not applicable to additional future research unless the authorization specifically and clearly states that the data will be used in the future for additional research.
        ii. Researchers are advised to use the Haring Center approved HIPAA Authorization template (but may use an equivalent form): https://www.washington.edu/research/forms-and-templates/template-hipaa- authorization/.

    b. When an IRB waives the requirement for patient authorization, in accordance with federal and state patient privacy laws, and all of the following conditions are met:
        i. The waiver or alteration of authorization document contains the following elements:
            a) The identity of the IRB (IRB federal registration number and local identifying name).
            b) The date on which the alteration or waiver of authorization was approved.
            c) A brief description of the PHI for which use or access has been determined to be necessary by the IRB or Privacy Board.
            d) Statement that the alteration or waiver of authorization has been reviewed and approved under either full IRB or expedited review procedures as follows:
                1) The IRB followed the requirements of the federal human subjects regulations, including the criteria for full or expedited

IRB review; *and*

2) The IRB chair or designee has signed the documentation of the alteration or waiver of authorization.

e) Statement that the IRB has determined that the alteration or waiver of authorization, in whole or in part, satisfies the following criteria:

1) Use or disclosure of PHI involves no more than minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

- An adequate plan to safeguard the identifiers from improper use and disclosure;
- An adequate plan to destroy the identifiers consistent with the conduct of the research and in accordance with retention policies, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; *and*
- Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted.

2) The research could not practicably be conducted without the alteration or waiver.

3) The research could not practicably be conducted without access to and use of PHI.

c. When the health information is de-identified prior to its release for research and the following conditions are met:

i. De-identification may be made by an individual who is designated and trained to perform this function, is either part of the Haring Center workforce or a business associate of Haring Center and is not a member of the research team to which the de-identified information will be provided.

d. Preparatory to research.

i. Preparatory to research activities are limited to research protocol preparation or other similar preparatory purposes and reviews to determine if there are sufficient numbers or types of records to conduct the research.

ii. UW Human Subjects Division (HSD) determines what constitutes research at UW and considers some activities categorized as “preparatory to research” to be research. For instance, HSD considers the review of PHI to identify possible research subjects and pilot studies to be research that requires IRB approval and either an IRB waiver of the HIPAA authorization requirement or the patient’s written authorization before the researcher may access PHI for this purpose. Accessing PHI does not only include direct access to the patient’s

medical records, but may also include other individually identifiable health records, and the collection or review of other data such as samples, specimens or autopsy materials.

iii. A Haring Center workforce member who is also a researcher may use Haring Center PHI preparatory to research if the researcher attests to the following:

a) The use of the PHI is solely to review it for the purpose of preparing a research protocol or planning the research activity. (For example, a researcher may review PHI to design a research study or to assess whether a sufficient number or type of records exist to conduct the research);
b) No PHI will be removed from the Haring Center covered entity by the researcher in the course of the review;
c) The PHI for which use is sought is necessary to prepare the research protocol or other similar preparatory purposes.

Receipt of or access to patient names and contact information to identify possible research participants requires IRB approval, including patient authorization or a waiver of HIPAA authorization.

C. Marketing Activities

1. Workforce members shall not use or disclose PHI for marketing without written patient authorization, except when the communication is in the form of:
   a. A face-to-face communication between a workforce member and the patient; *or*
   b. A promotional gift of nominal value provided by Haring Center.

2. If the marketing involves financial remuneration to Haring Center from a third party, the patient authorization must state that such remuneration is involved.
3. The following types of communications from Haring Center to patients are not consideredto be marketing (unless Haring Center receives financial remuneration in exchange for making the communication):
   a. Communications to describe health-related products or services (or payment for such products or services);
   b. Communications about a patient's treatment, health-related products or services, case management or care coordination;
   c. Refill reminders or other communications about a patient's current prescriptions for drugs or biologics (if Haring Center receives financial remuneration in exchange for making the communication and the remuneration is reasonably related to the cost of making the communication, it is not considered to be marketing);

   d. Directives or recommendations for alternative treatments, therapies or healthcare professionals, or for settings of care for the patient. For example, it is not marketing when a physician describes and refers a patient to the services offered by another Haring Center healthcare professional specializing in care

that is appropriate to the patient's treatment plan.

II. Authorizations for the Use or Disclosure of PHI

A. Valid Authorization

Except as defined below, a signed patient authorization is not a waiver of any rights a patient has under other statutes, the rules of evidence or common law.

1. A valid authorization to allow use and disclosure of PHI shall be written in plain language and contain at least the following core elements:
   a. The patient's name, signature and date, or the signature and date of the patient's personal representative or surrogate decision maker;
   b. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
   c. The name or other identification of the person(s) or class of persons, agency, or organization authorized to make the requested use or disclosure;
   d. The name or other identification of the person(s) or class of persons, agency, or organization to whom Haring Center is authorized to make the requested disclosure;
   e. A description of each purpose of the requested use or disclosure (a workforce member may add the statement "at the request of the patient" when a patient initiates the authorization and does not, or elects not to, provide a statement of the purpose);

   f. An expiration date or an expiration event that relates to the patient or the purpose of the use or disclosure;
      i. Where the patient is under the supervision of the department of corrections, an authorization signed pursuant to this section for healthcare information related to mental health or drug or alcohol treatment expires at the end of the term of supervision; unless the patient is part of a treatment program that requires the continued exchange of information until the end of the period of treatment;
   g. A statement of the patient's right to revoke the authorization in writing, the exceptions to the patient's right to revoke the authorization, and a description of how the patient can make a revocation;
   h. A statement that Haring Center will not condition treatment or payment based on the patient's provision of an authorization for the requested use or disclosure, **except**:
      i. Haring Center may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of PHI for such research; *or*
      ii. Haring Center may condition the provision of healthcare that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party;

i. A statement that when the information is used or disclosed in accordance with a signed authorization, it may be subject to re-disclosure by the recipient and may no longer be protected by state and federal laws protecting healthcare information; *and*

j. If the authorization is signed by the patient's personal representative or surrogate decision maker, the authorization shall include a description of the signatory's authority.

2. Certain types of PHI are entitled to heightened confidentiality. Workforce members shall not disclose these types of PHI unless the authorization explicitly documents the patient's authorization to release them. These types of PHI include information about:

    - STDs, including but not limited to AIDS or HIV;
    - Behavioral or mental health services; *and*
    - Treatment for alcohol or drug abuse.

    a. When disclosure of the above types of PHI about patients is not for TPO purposes, workforce members shall add a written confidentiality statement to the authorization form addressing the prohibition of re-disclosure of any PHI. The statement must include the following or substantially similar language:

    "This information has been disclosed to you from records whose confidentiality is protected by state law. State law prohibits you from making any further disclosure of it without the specific written authorization of the person to whom it pertains, or as otherwise permitted by state law. A general authorization for the release of medical or other information is NOT sufficient for this purpose."

    b. If the non-TPO disclosure is made verbally, the same written confidentiality statement as above is required; the workforce member shall send the statement within 10 days of the disclosure. Whenever a workforce member makes a verbal disclosure of PHI related to STDs, the workforce member must complete an authorization that captures all required information and add it to the patient's designated record set.

3. The authorization may contain other elements or information if not inconsistent with Section V.A. of this policy.

B. Invalid Authorizations

An authorization is invalid under any of the following circumstances:

1. The authorization lacks one of the required core elements of a valid authorization as defined in Section V.A of this policy;
2. The expiration date has passed or the expiration event is known by Haring Center to have occurred;
3. Haring Center is aware that the authorization has been revoked by the patient;

4. The authorization violates the prohibitions stated in Section V.C of this policy;
5. A Haring Center workforce member receives an authorization that contains information that the workforce member knows to be false;
6. The patient makes any revisions or alterations to the required core elements of the authorization form.

C. Prohibition on Conditioning of Authorizations

Workforce shall not condition provision of individual treatment or payment on the provision of an authorization **except** in the following situations:

1. Research-related treatment may be conditioned on provision of an authorization for the use or disclosure of PHI for such research; *or*
2. Healthcare that is solely for the purpose of creating PHI for disclosure to a third party may be conditioned on provision of an authorization for the disclosure of the PHI to such third party.

D. Compound Authorizations

An authorization for use or disclosure of PHI shall not be combined with any other document **except** in the following situations:

1. An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. This includes creating a compound authorization for the use or disclosure of PHI for a research study with:

    a. Another authorization for the same research study,
    b. An authorization for the creation or maintenance of a research database or repository, *or*
    c. A consent to participate in research.
    Where Haring Center has conditioned the provision of research-related treatment on the provision of one of the authorizations, any compound authorization created shall clearly differentiate between the conditioned and unconditioned components. For the unconditioned components, workforce members shall provide the patient with an opportunity to opt in to the research activities described in the authorization.

2. For psychotherapy notes, authorization for use or disclosure may only be combined with another authorization for a use or disclosure of psychotherapy notes.

E. Processing Authorizations

1. When a patient provides written authorization for a use or disclosure, workforce members shall adhere to the conditions and limitations of the authorization.
2. Authorization forms shall be directed to the applicable HIM department for processing.

3. Haring Center shall act upon all authorizations within 15 working days as required by state law.
4. Haring Center shall provide the patient with a copy of the signed authorization.
5. Haring Center shall document and retain in electronic or written format all signed authorizations and actions taken in response to the authorizations in the designated record set.

F. Revocation of Authorizations

Patients (or their personal representatives or surrogate decision makers) may revoke authorizations in writing at any time **unless**:

1. Haring Center has already taken substantial action based on the original authorization; *or*
2. The authorized use or disclosure is necessary for Haring Center to be compensated for treatment already provided to the patient.

A patient's revocation instruction shall be shared with all impacted HIM departments.

Special Circumstances

De-Identification of PHI

Federal and state laws do not protect health information that does not identify an individual and cannot be used to identify an individual.

1. Requirements for de-identification of PHI

One of the following two methods shall be used to demonstrate that PHI is de-identified:

a. Method One. A workforce member removes all of the following eighteen (18) identifiers of the patient or of the patient's relatives, employers or household members, provided that the workforce member does not have knowledge that the information could be used alone or in combination with other information to identify the patient. The eighteen (18) identifiers are:

i. Names;
ii. All geographic subdivisions smaller than state including:
   a) Street Address
   b) City
   c) County
   d) Precinct
   e) Zip code and equivalent geo code
      except if the initial three digits of a zip code:

         1) Represents a geographic unit in which combining all zip codes with the same 3 initial digits contains more than 20,000 people; *and*

         2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are

changed to "000."

iii. All elements of dates (except year) directly related to an individual including:
   a) Birth date;
   b) Admission date;
   c) Discharge date;
   d) Date of death; *and*
   e) All ages over 89, including date elements indicative of such age, including year, except when all ages of 90 or older can be aggregated into a single category;

iv. Telephone numbers;
v. Fax numbers;
vi. E-mail addresses;
vii. Social security numbers;
viii. Medical record numbers;
ix. Health plan beneficiary numbers;
x. Account numbers;
xi. Certificate/license numbers;
xii. Vehicle identifiers and serial numbers (including license plate numbers);
xiii. Device identifiers and serial numbers;
xiv. Web universal resource locators (URLs);
xv. Internet protocol (IP) address numbers;
xvi. Biometric identifiers, including finger/voice prints;
xvii. Full face photographic images and any comparable images; *and*
xviii. Any other unique identifying number, characteristic or code;

b. Method Two**.** A person with appropriate knowledge and experience applying generally accepted statistical and scientific methods for rendering information not individually identifiable:

   i. Applies such principles/methods;
   ii. Determines the risk is very small that the information could be used alone or in combination with other available information to identify an individual; *and*
   iii. Documents the methods and results of the analysis that justify the determination.

2. Re-identification requirements

A workforce member may assign a code or other means of record identification to allow information that has been de-identified through Method One or Two in Section VI.B.1 above to be re-identified, provided that the following two conditions are met:

a. The code or other means of record identification is not derived from or related to information about the patient and cannot otherwise be translated to identify the patient; *and*

b. The workforce member does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism used for re- identification.

The workforce member determines where to maintain the codes for re-identification and how they are secured.

Inappropriate use or disclosure of the code or other means of record identification may constitute a disclosure of PHI and may trigger a breach or violation of a data use agreement.

B. Public Records Requests

Members of the public may make requests for information from the University through the UW Office of Public Records. If the Office of Public Records receives a request for Haring Center information, the Office of Public Records works with the appropriate Haring Center contact to process the request. Haring Center shall comply with state and federal patient privacy laws when responding to such requests.

There are three options when processing a public records request that includes patient information:

1. If the request is for an individual's patient medical record, the Office of Public Records refers the requestor to the appropriate health information management department. These types of requests require a valid authorization.
2. If there is a reasonable basis to believe that the requested information can be used to identify a Haring Center patient(s) (a relative, the employer or a household member of the individual patient) the information cannot be provided to the requestor without a valid patient authorization. The workforce member shall inform the requestor that the information cannot be released because it might lead to identification of Haring Center patients (or a relative, the employer or a household member of the individual patient), and that authorization from those unnamed patients is required for release.
3. If the request is for multiple patients or information that contains multiple patients' information, the patient information must be de-identified before it is released. In processing the request, the entity contact highlights the information that may need to be redacted before it is sent to the Office of Public Records. The Office of Public Records reviews the information to ensure that all appropriate individual identifiers are redacted before it is released to the requestor. Workforce members shall use the following guiding principles when reviewing the information:
    - De-identify all information about individuals if they cannot be clearly identified as workforce members on the job or if there is evidence to conclude that:
        - The individual is seeking care;
        - It is a relative of an individual seeking care;
        - It is an employer of an individual seeking care; *or*
        - It is a household member of an individual seeking care.

SANCTION POLICY

Applicability: UW Healthcare Components

Policy Title: Corrective Actions

Policy Number: HCCG.001

Date Established: January 24, 2024

Date Effective: April 01, 2024

Next Review Date: January 24, 2025

PURPOSE

This policy obligates UW Healthcare Components Group to address compliance violations with appropriate and timely corrective actions. It applies to all designated institutional officials in UW Healthcare Components Group who have responsibility for enforcement, discipline and corrective actions. This includes leaders, managers, chairs, supervisors, disciplinary boards and councils, and constituent-specific officials (for example, residing in human resources, academic personnel, graduate medical education, student affairs, etc.).

Background

The University operates as a hybrid entity as defined by the U.S. Department of Health and Human Services Office of Civil Rights Health Insurance Portability and Accountability Act (HIPAA) Regulations. The hybrid entity's designated functions at the university adhere to HIPAA and Washington State Department of Health Regulations.

UW Healthcare Components Group (HCCG) performs functions that support UW's operation as a hybrid entity, including functions that support UW's HIPAA covered entities. As such, the HCCG workforce adheres to HIPAA and Washington State Department of Health Regulations.

A covered entity must have a variety of appropriate sanctions available and apply appropriate sanctions for individuals affiliated with the University who fail to comply with the policies and procedures of the covered entity.

DEFINITIONS

Covered Entity

Healthcare organizations and other types of organizations/entities to which the HIPAA Regulations apply.

Electronic Protected Health Information (ePHI)

Refers to any protected health information (PHI) that is covered under HIPAA security regulations and is produced, saved, transferred, or received in an electronic form.

Health Insurance Portability and Accountability Act (HIPAA)

(HIPAA is a set of federal regulations that apply to healthcare providers which engage in certain electronic transactions, health plans, and healthcare clearing houses (aka covered entities).

Protected Health Information (PHI)

Refers to any protected health information (PHI that is covered under HIPAA security regulations. PHI is any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a healthcare service, such as a diagnosis or treatment.

Workforce

Employees, staff, healthcare professionals including those credentialed through the entity medical staff offices (physicians and non-physician providers), faculty, residents, fellows, students, trainees, observers, visiting scholars, volunteers, researchers, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, including temporary workers, whether or not they are paid by the covered entity or business associate.

For purposes of HIPAA compliance, workforce also includes individuals, whose conduct in the performance of work for the UW Healthcare Components Group or a Business Associate (or government agency contracted under a Memorandum of Understanding), is under the direct control of the UW Healthcare Components Group or business associate/government agency, whether or not they are paid by the Covered Entity or business associate/government agency.

(Source: 45 C.F.R. §160.103)

(See also UW APS 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions for UW applicability.)

POLICY

All findings of noncompliance established by staff in the Compliance Department with scope and jurisdiction over the issue result in the application of appropriate corrective actions, by a designated institutional official[i], involving one or more of the following:

- Required/appropriate notifications;
- Process improvements;
- Claim corrections;
- Repayments;
- Changes to the terms and conditions of a workforce member's relationship with UW Healthcare Components:
    - Disciplinary actions or sanctions, up to and including termination of the workforce member's relationship with UW Healthcare Components;
    - Changes in staffing;

    - Contract termination;
- Issuance of an advisory;
- Re-education and training; *and/or*
- Other appropriate corrective action.

Designated institutional officials consider the following factors in determining what corrective actions are appropriate for workforce members:

- Prior violations and sanctions;
- The nature, severity and extent of the violation;
- Whether the violation is a result of conduct that is intentional, willful or with reckless disregard for the law;
- Terms and conditions of the workforce member's relationship with UW Healthcare Components, as determined by constituent-specific policies, state regulations, conduct codes and applicable guidelines; *and*
- Whether or not the violation was self-reported (self-reporting does not exempt a workforce member from corrective action but will be taken into account).

Designated institutional officials maintain all documentation associated with corrective actions in accordance with UW Healthcare Components constituent-specific record retention policies.

REGULATORY/LEGISLATION/REFERENCES

- United States Sentencing Commission, Guidelines Manual, §8B2.1 (Nov. 2016).
- Employee Education About False Claims Recovery, Deficit Reduction Act of 2005 § 6032 (codified at 42 U.S.C. § 1396a(a)(68)).
- Relief from Retaliatory Actions, Federal False Claims Act, 31 U.S.C. §3730(h).
- 45 CFR – Part 164 Public Welfare. Subchapter C - Administrative Data Standards and Related Requirements
- HIPAA Administrative Simplification Regulation Text 45 CFR Parts 160, 162, 164Download pdf

APPROVALS

/s/ Jane Yung _____ Jane Yung
Executive Director, CRS
UW Privacy Official

_____
Date

[i] Violations of federal or state laws may also be subject to criminal prosecution, fines, imprisonment and/or exclusion from participation in federally sponsored healthcare programs.