

**STUDENT CLINICIAN REQUEST TO ACCESS ePHI OFF-SITE
And Remote User's Access Agreement and Attestation**

This form is required for approval to:

- Access any system containing ePHI from any location other than the SCCE building.
- Receive a CEHS/SCCE-issued device to be used for SCCE work-related purposes.

Please complete the form and e-mail it to joni.black@usu.edu. This form must be approved before you will be issued a device and before you may access any ePHI system from off-site.

Section One- Workforce Data

First Name _____ MI _____ Last Name _____
Phone Number _____ USU E-mail Address _____

Department _____ Clinic Name _____ Clinical Supervisor _____

If working in more than one clinic:

Department _____ Clinic Name _____ Clinical Supervisor _____

Have you read the policy "Accessing ePHI Remotely"? Yes ☐ No ☐

Is this request for (check one);

Purpose of accessing systems from off-site (already have a CEHS/SCCE-issued device) ☐

Purpose of accessing systems from off-site and receiving a CEHS/SCCE-issued device ☐

Section Four- Device and Software Information

Do you have an existing CEHS-issued laptop or other device that you will be using for SCCE clinical work? Please check "no" if you need to be assigned a CEHS device. Y ☐ N ☐

If you already have a CEHS-issued device, has this device been determined to meet CEHS security standards for clinical work by the CEHS IT department? Y ☐ N ☐ Not Sure ☐

Section Five- Remote User's Access Agreement and Attestation

I attest, by my signature, that I will abide by all CEHS HIPAA Privacy and Security policies and procedures, including the Accessing ePHI Remotely policy.

- I assure that I will only access ePHI systems in a private, secure physical space.
- I agree to log on to the USU Staff VPN before accessing any ePHI systems from my device.
- I will only use devices that have been issued and approved by CEHS IT.
- I will not share my password(s), log in information or CEHS/SCCE-issued device with anyone.
- I will log off of ePHI systems and lock my device when I am not using it.
- I will not configure my device to auto save passwords to ePHI systems.
- I will not copy any confidential information, including ePHI to any media. I will not print or use paper copies of PHI off-site.
- I will only send emails containing ePHI if the email is properly encrypted.
- I will immediately report a lost or stolen device to the SCCE Compliance Officer and CEHS IT.



- I will report any known or suspected impermissible use, access, acquisition or disclosures of PHI to the SCCE Compliance Officer.
- I understand it is my responsibility to meet these requirements.

Signature

Date

Section Six- Approvals

Clinic 1 Supervisor Signature

Date

Clinic 2 Supervisor Signature (if applicable)

Date

SCCE Administrator Signature

Date

SCCE Compliance Officer Signature

Date

Admin Use Only

Comments