

POLICY INFORMATION

Document # 3001	Title: Accessing ePHI Remotely	Original Effective Date: 06.22.2021
Safeguard: Security	Approved by: Gretchen Peacock	Review Date:

I. POLICY STATEMENT

CEHS recognizes that there may be circumstances where offsite/remote work needs to occur. This policy establishes guidelines and defines standards for remote access to ePHI information resources (networks, systems, applications, and data including but not limited to electronic Protected Health Information (ePHI) received, created, maintained, or transmitted by the Health Care Components (HCCs)). Remotely accessing ePHI is a privilege and is granted only to remote users who have a defined need for such access and demonstrate compliance with CEHS's safeguards that protect the confidentiality, integrity, and availability of information resources. These safeguards have been established to address HIPAA security regulations. The guidelines outlined in this policy are designed to minimize exposure to damages that may result from unauthorized use of USU, CEHS, and SCCE resources and confidential information.

II. DEFINITIONS

See HIPAA Policy 100

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units listed as a hybrid entity according to USU's HIPAA Hybrid Covered Entity Declaration. Only the health care components (HCC) (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

IV. PROCEDURES TO IMPLEMENT

1. REMOTE ACCESS REQUEST AND APPROVAL

- a. Workforce members shall request permission to access ePHI remotely by completing the "Accessing ePHI Remotely" request form (See Attachment A). Permission to access ePHI remotely is granted only to workforce members with a defined business need, at the discretion of the workforce member's supervisor, and with approval by the SCCE Executive Director and Security Officer or designee.



- b. The workforce member is responsible for adhering to all of CEHS and SCCE's policies and procedures.
- c. Workforce members granted remote access privileges must sign and comply with the "Confidentiality Agreement" along with the "Remote User's Access Agreement" (See Attachment A).
- d. The remote access user's responsibility is to ensure that the remote worksite meets privacy and security standards established by CEHS and SCCE. This includes the configuration of personal routers and wireless networks.

2. EQUIPMENT, SOFTWARE, AND HARDWARE

- a. CEHS and SCCE will not provide all equipment or supplies necessary to ensure proper information protection to which the user has access. The following assists in defining the equipment and environment required.
 - i. CEHS/SCCE provided:
 - 1. Encrypted Device
 - 2. VPN Access
 - ii. User provided:
 - 1. Internet connection and fees
 - 2. Secure workspace environment isolated from visitors, family, others.
- b. Only CEHS-issued devices or devices approved through CEHS IT may be used for remote access.

3. SECURITY AND PRIVACY

- a. Only authorized remote users are permitted remote access to any of CEHS and SCCE's ePHI systems must adhere to all of CEHS's policies.
- b. Remote users must log in to the USU Staff VPN before accessing any CEHS or SCCE systems containing sensitive information.
- c. It is the responsibility of the remote access user to log off and disconnect from USU's network when access is no longer needed to perform job responsibilities.
- d. It is the responsibility of the workforce member to ensure that unauthorized individuals do not use CEHS/SCCE-issued devices. At no time will any user share their username or password with anyone, nor configure their device to remember or automatically enter their username and password.
- e. Remote users must take necessary precautions to secure all equipment and information in their possession.
- f. Copying confidential information, including ePHI, to any media is strictly prohibited.



- g. CEHS IT and USU IT maintain logs of all activities performed by remote access users while connected to USU's network. System administrators review this documentation and use automated intrusion detection systems to detect suspicious activity. Electronic Protected Health Information system accounts that have shown no activity for longer than 60 days may be disabled.
- h. Remote users are not allowed to use or print paper documents that contain PHI.
- i. Users may not send any ePHI via email unless it is encrypted and a USU (first name.last name@usu.edu) email account is used.
- j. Internet of Things (IoT): Voice-activated devices (such as Alexa/Echo, etc.) should be disabled when communicating via teleconferencing or in confidential conversations regarding SCCE clients.

4. ENFORCEMENT

- a. Remote access users who violate this policy are subject to sanctions and disciplinary actions, including termination.

V. ATTACHMENTS

- A. Student Clinician Request To Access ePHI Off-Site And Remote User's Access Agreement and Attestation

VI. REFERENCES

N/A

VII. PREVIOUS REVIEW INFORMATION

Review Date	Reviewed by	Approved by
-------------	-------------	-------------

ATTACHMENT A

**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 Sign

Date

SCCE Compliance Officer Signature

Date

Admin Use Only

Comments