**TS – A (1 & 2) Access Control**

***Purpose***

To implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a).

**Guidance**

Ensure the verification of the individual or entity that is authorized to access ePHI and that the identity is correctly bound to a unique user identification (“sign-on”) for access to ePHI.

* Each user must be provided a unique account, with a unique username/userID and password, for access to ePHI.
* Generic or shared accounts are not permitted for access to ePHI.

**Unique User Identification**

Assign a unique name and/or number for identifying and tracking user identity. 164.312(a)(2)(i)

**Emergency Access Procedure**

Implementation: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. 164.312(a)(2)(ii)

Establish procedures to ensure that necessary ePHI can be accessed during an emergency.

* Emergency access procedures may be included in Contingency Plan procedures (see [*§164.308(a)(7)(i) - Contingency plan*](https://its.ucsc.edu/policies/hipaa-practices.html#308a7i)*)*.
* The emergency access procedures shall be written and communicated in advance to multiple individuals within the organization.
* Emergency access procedures should not rely on the availability of a single individual.
* Access to emergency procedures should not rely on the availability of local power or network.
* Identify roles that may require special access during an emergency.
	+ Individuals are to require proper ID or other official verification before granting access to unknown or not-normally-authorized individuals in emergency circumstances.

**Automatic Logoff**

Implementation: incorporate electronic procedures that terminate an electronic session after a predetermined time of inactivity. 164.312(a)(2)(iii)

* Where possible, terminate electronic sessions after a period of inactivity.
* Where session termination is not possible, either from a technical solution or from a business process perspective, implement automatic workstation lockout as a compensating control.
* Maximum duration of inactivity prior to session termination or automatic workstation lockout is 10 minutes. *Note: The UofL Information Security Office/Privacy Office may consider requests for exceptions to the 10-minute requirement.*

**Encryption and Decryption**

Implementation: add a mechanism to encrypt and decrypt electronic protected health information. 164.312(a)(2)(iv)

**Note:**the scope of this implementation specification to include stored ePHI. See 164.312(e)(2)(ii) – Encryption, below, for transmission of ePHI.

* Implement appropriate security measures, such as encryption, to protect ePHI from unauthorized access.
* Implement appropriate security measures, such as encryption, to protect ePHI from unauthorized access.
	+ Unencrypted ePHI will not be stored on portable electronic devices, including laptops (see [*§164.310(b) - Workstation use*](https://its.ucsc.edu/policies/hipaa-practices.html#310b) and [*§164.310(c) - Workstation security*](https://its.ucsc.edu/policies/hipaa-practices.html#310c)).
* In situations where encryption is problematic, the alternative compensating controls below must be implementedas appropriate, in consultation with the UofL IT Enterprise Security Team.
	+ An explanation must be provided for why encryption is not being implemented.

***Alternative, reasonable and appropriate compensating controls if encryption is not in place for stored ePHI:***

* Access controls, including unique user ID & password authentication, and user profiles (SHS only)
* Hardening of systems (see [*§164.308(a)(5)(ii)(B) - Protection from malicious software*](https://its.ucsc.edu/policies/hipaa-practices.html#308a5iib) for details)
* Physical security for access to facilities and workstations that contain or access ePHI, including appropriate device and media controls
* Technically enforce complex passwords where possible
* Enable system security auditing/logging, including monitoring of audit reports/logs
* Correct configuration of applications to use secure protocols
* Implement automatic logoff and/or screen lock (see [*§164.312(a)(2)(iii) - Automatic logoff*](https://its.ucsc.edu/policies/hipaa-practices.html#312a2iii) for details)
* Ensure secure remote access
* Implement correctly configured firewalls (hardware and/or software)