**TS – D Person or Entity Authentication**

***Purpose***

To implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. 164.312(d)

**Guidance**

* Each User must be provided a unique account, with a unique username and password, for access to ePHI.
	+ Generic or shared accounts are not permitted for access to ePHI.
	+ Passwords for access to ePHI will not be shared by UCSC employees.
	+ All passwords providing access to ePHI, including local administrator/root passwords, must comply with the password strength requirements in [UofL’s *Password Strength and Security Standards*](https://sharepoint.louisville.edu/sites/policies/library/SitePages/Information%20Technology/Passwords.aspx)*.*
	+ Physically protect passwords (see UCSC's*Password Strength and Security Standards*, link above).
* Review, as appropriate, workstation, OS and application access logs, as well as failed or successful changes to account permissions (also see [*§164.308(a)(1)(ii)(D) - Information system activity review*](https://its.ucsc.edu/policies/hipaa-practices.html#308a1iid)).
* Systems and applications will not be configured to save passwords.
* All of the above practices apply to vendors and third parties.