**TS – E (1 & 2) Transmission Security**

***Purpose***

To implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. 164.312(e)(1)

**Guidance**

* Wired and wireless transmission of ePHI will utilize secure protocols (encryption).
  + All remote access of ePHI must be by secure methods only.
* Unprotected ePHI shall not be sent via unencrypted email.
  + Note: It is acceptable to send ePHI via email in encrypted, password-protected attachments to known business partners, UCOP, and in response to legitimate requests if no secure channel exists.
* Received email containing ePHI must be adequately deleted when there is no longer a business need to retain it. Procedures are available in individual HIPAA entity training or in the [IT Request Knowledge Base](https://ucsc.service-now.com/kb_view.do?sysparm_article=KB0016804).
* Employees must delete or redact ePHI from the body of received email before replying to it.

**Integrity Controls**

Implementation: Incorporate security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. 164.312(e)(i)

**Encryption**

Implementation: Incorporate a mechanism to encrypt electronic protected health information whenever deemed appropriate.

See §164.312(e)(2)(i) - Integrity controls, above, for recommended practices.

Note: Also see §164.312(a)(2)(iv) – Encryption and decryption, above, for stored ePHI.