hipaa security rule language: “implement a mechanism to encrypt ephi whenever deemed appropriate.”

regulatory reference: 45 cfr 164.312(e)(2)(ii)

i. purpose

this standard reflects east carolina university’s commitment to appropriately use encryption to protect the confidentiality, integrity and availability of ephi transmitted over electronic communications networks.

ii. authorization and enforcement

health care component management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the ecu it security officer, ecu hipaa security officer, and ecu hipaa privacy officer.

iii. standard

appropriate encryption must be used to protect the confidentiality, integrity, and availability of ecu ephi transmitted over electronic communications networks.

iv. applicability

this standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. a healthcare computing system is defined as a device or group of devices that store ephi which is shared across the network and accessed by healthcare workers.
V. PROCEDURE

1. ECU Health Care Components must consider the following factors at a minimum in determining whether or not encryption must be used when sending specific EPHI over an electronic communications network:

   - The sensitivity of the EPHI
   - The risks to the EPHI
   - The expected impact to ECU functionality and work flow if the EPHI is encrypted
   - Alternative methods available to protect the confidentiality, integrity and availability of the EPHI

VI. COORDINATING INSTRUCTIONS

1. All section policies and procedures will be reviewed annually. Every section policy and procedure revision/replacement will be maintained for a minimum of six years from the date of its creation or when it was last in effect, whichever is later. Other East Carolina University, University of North Carolina system, or state of North Carolina requirements may stipulate a longer retention period.