Technical Safeguards

45 CFR Subtitle A, Subpart C – Security Standards for the Protection of Electronic Protected Health Information

§164.312 Technical Safeguards.

A covered entity or business associate must, in accordance with §164.306 [*Security Rule General Rules*]:

(a) (1) *Standard: Access control*. 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)(4). [*Standard: Information access management*. *Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E [Privacy Rules] of this part.*]

(2) *Implementation specifications:*

(i) *Unique user identification (Required)*. Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure (Required).* Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) *Automatic logoff (Addressable)*. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) *Encryption and decryption (Addressable)*. Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c) (1) *Standard. Integrity.* Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) *Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)*. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e) (1) *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications:*

(i) *Integrity controls (Addressable)*. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) *Encryption (Addressable)*. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]