HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) SECURITY RULE SUMMARY - 45 CFR Part 164 Subpart C

SECTION 1: General Rules

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI (Electronic Protected Health Information).

(1) Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;

(2) Identify and protect against reasonably anticipated threats to the security or integrity of the information;

(3) Protect against reasonably anticipated, impermissible uses or disclosures; and

(4) Ensure compliance by their workforce.

SECTION 2: Technical Safeguards (164.312)

(a) 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.

  - Unique User Identification (Required): Assign a unique name and/or number for identifying and tracking user identity.

  - Emergency Access Procedure (Required): Establish (and implement) as needed, procedures for obtaining necessary electronic protected health information during an emergency.

  - Automatic Logoff (Addressable): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

  - Encryption and Decryption (Addressable): Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) 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) Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(d) 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) 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.