

Data Security Policy – ePHI Safeguards

PURPOSE

To provide principles and guidelines for protecting and safeguarding ePHI and other sensitive or protected information.

SCOPE

The ePHI Safeguards Policy will cover Organization's:

- Obligations for safeguarding ePHI and other sensitive or protected information
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY/PROCEDURES

Organization has adopted and follows processes for protecting *ePHI* and other sensitive or protected information from tampering or unauthorized access. The company safeguards the confidentiality, integrity, and availability (CIA triad) of ePHI that Organization creates, processes, receives, or transmits.

Organization only permits authorized access to *ePHI* and systems that contain *ePHI*.

Organization has set up processes and security mechanisms to ensure that *ePHI* is properly transmitted and encrypted.

VIOLATIONS

Noncompliance with the HIPAA Security Rule or violation of ePHI safeguards may result in disciplinary action or sanction.

RELATED POLICY

- Data Security – Device and Media Control Policy

RELEVANT HIPAA REGULATIONS:

- [45 CFR 164.312\(a\)\(2\)\(iv\)](#) *Encryption and Decryption*
- [45 CFR 164.312\(e\)\(2\)\(ii\)](#) *Encryption*
- [45 CFR 164.310\(d\)](#) *Device and Media Controls*