Data Security Policy – Transmission Security

PURPOSE

To provide principles and guidelines for protecting data-in-transit and secure data transmission.

SCOPE

The Transmission Security Policy will cover Organization's:

- Data transmission safeguards
- Secure data transmission
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has adopted and follows security measures to protect the confidentiality and integrity of sensitive and protected information, such as ePHI, that is transmitted over a network.

Any sensitive or protected data transmitted over a network must be protected from unauthorized access or disclosure. Data transmission safeguards must also prevent modification or corruption, or alert in the event of data modification or corruption.

Organization requires the following security measures for sensitive or protected data-in-transit, including ePHI:

- Sensitive or protected data, including ePHI, must be securely encrypted during transmission unless explicitly requested in writing by the patient
- Remote access to ePHI must be secure, such as over a Virtual Private Network (VPN)
- End-to-end email encryption

Encryption methods used to protect data-in-transit should be up-to-date and secure, such as TLS 1.2+.

Employees must avoid sending ePHI and other sensitive or protected information through insecure or unapproved mechanisms except in very limited circumstances as required under HIPAA upon the request of an individual. In those instances, transmission should only be after consultation with the security officer.

PROCEDURES

Organization requires certain controls and safeguards for the transmission of sensitive or protected data or information over a network. The company requires all data-in-transit to be encrypted and use secure protocols, such as TLS1.2+.

Remote access to ePHI is only permitted through a VPN or other approved secure connection mechanism.

ePHI will not be sent over unencrypted email unless explicitly requested in writing by the patient. Patients requesting unencrypted ePHI over email should be informed that this is not a secure method of communication. Any ePHI sent via email should be redacted in replies.

Workforce members are prohibited from sending ePHI and other sensitive or protected information using insecure or unapproved methods except in very limited circumstances as required under HIPAA upon the request of an individual. In those instances, transmission should only be after consultation with the security officer.

Encryption

Organization has set up processes and safeguards to encrypt

- Data-at-rest
- Data-in-transit
- Files, data, and devices that store or process sensitive or protected information, including ePHI
- Emails containing ePHI
- Other devices, disks, and systems

RELEVANT HIPAA REGULATIONS

- §164.312(e)(1) *Transmission security*
- §164.312(e)(2)(i) *Integrity controls*
- §164.312(e)(2)(ii) *Encryption*

RELEVANT SOC 2 CRITERIA

- CC6.1.2 *Restricts logical access*
- CC6.6.2 *Protects identification and authentication credentials*
- CC6.7.1 *Restricts the ability to perform transmission*
- CC6.7.2 *Uses encryption technologies or secure communication channels to protect data*
- CC6.8.5 *Scans information assets from outside the entity for malware and other unauthorized software*