

# POLICY & PROCEDURE

<b>Practice:</b> Organization Name	<b>Effective Date:</b> April 14, 2005
<b>Title:</b> Electronic Transmission Security of PHI	<b>Date Revised:</b> April 14, 2005
<b>Policy Number:</b> 2245	<b>Reference:</b> 45 CFR § 164.312(e)(1) + (2)

## **TITLE: ELECTRONIC TRANSMISSION SECURITY OF PHI**

**RESPONSIBILITY:** Security Official and Director of Information Systems

## **BACKGROUND:**

Electronic protected health information while in transit is subject to risk of interception and unauthorized access. However, as it is transmitted, [ENTITY] must take precautions to protect the data. Such precautions should address the need to protect the data in strength equal to the level of risk associated with such data.

## **POLICY:**

[ENTITY] maintains a comprehensive internal security control program coordinated by the Information Systems Department to guard against unauthorized access to electronic protected health information. [ENTITY] uses a combination of operational practices and technological solutions to ensure the confidentiality, integrity, and availability of protected health information while it is in transit from one location to another location over an electronic communications network. This type of electronic transmission or movement of protected health information includes at a minimum:

1. Use of an electronic communications network/local area network
2. Point to point transmission along an open network (such as the internet)
3. Use of dial up lines
4. Email
5. Fax (NOTE: There are two kinds of facsimile. This policy applies to facsimile originating from computer based software applications).

## **PROCEDURE:**

The Security Official will gather all information collected for the risk assessment process relating to all areas of electronic transmission security. This assures that the processes chosen to carry out the security of electronic transmission are in accordance with the level of risk, priority, and importance assessed by [ENTITY].

1. The Security Official will establish a committee comprised of the following (as necessary and applicable), or their designees:
  - a) Designated Security Official (*chair*)
  - b) Designated Privacy Official
  - c) Director of Information Systems
  - d) Director of Human Resources
  - e) Facilities Maintenance
  - f) Representatives from affected business areas

# POLICY & PROCEDURE

<b>Practice:</b> Organization Name	<b>Effective Date:</b> April 14, 2005
<b>Title:</b> Electronic Transmission Security of PHI	<b>Date Revised:</b> April 14, 2005
<b>Policy Number:</b> 2245	<b>Reference:</b> 45 CFR § 164.312(e)(1) + (2)

2. The committee is responsible to choose the [ENTITY] preferred combination of process and technical solution(s) to develop the procedures which function to reasonably safeguard [ENTITY] protected health information, and make up secure transmission protocol by considering the following factors:
- Reviewing the risk assessment results and related documentation
  - Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.
  - Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability
  - Thoroughly considering all areas defined in the procedure as "Implementation Considerations"

## Implementation Considerations Relating to Transmission Security

Consider the business needs for transmission security:

- [ENTITY]'s need to send electronic PHI over an electronic communications network to providers/brokers/patients/ business associates/employees, and others. This should include: transmission of PHI over public networks, private networks, and wireless networks.
- [ENTITY]'s need to allow others such as employer, or customer support functions remote access
- Consider processes used to gain access:
  - Dial-up modem
  - Virtual or dedicated private network
  - Extranet Virtual Private Network
  - Wireless Encryption and authentication methods
  - IPsec communications

## Closed Enterprise Network Controls

All communications access to [ENTITY] from an open network, such as the Internet and untrusted third party networks, requires strong authentication.

Communication protocols that will be used when transmitting to and from the [ENTITY] include integrity and authenticity of the information (See related technical policies).

## Network Perimeter Controls

All access points to untrusted networks shall use some type of security mechanism which could include, but not limited to: Firewalls, network address translation device, gateways, and proxies

# POLICY & PROCEDURE

<b>Practice:</b> Organization Name	<b>Effective Date:</b> April 14, 2005
<b>Title:</b> Electronic Transmission Security of PHI	<b>Date Revised:</b> April 14, 2005
<b>Policy Number:</b> 2245	<b>Reference:</b> 45 CFR § 164.312(e)(1) + (2)

## Network services and the general public

General public access to [ENTITY] information is only via connection in a secure manner.

## Encryption Controls

Encryption and decryption use allows for information to be scrambled so that if it were intercepted, it would not be easily understood. It is important for [ENTITY] to determine what level of data is worthy of encryption since overuse can prove financially and technically burdensome. Whenever encryption and decryption is used, the following should be addressed:

- d) Definitive level of algorithm strength
- e) Procedure for key generations
- f) Key reproduction for emergency access
- g) Distribution, storage, use, destruction, and archiving of keys
- h) Some common methods of encrypting data in transit include:
  - i. SSL
  - ii. IPSEC
  - iii. Public/Private Key Encryption
  - iv. VPN
  - v. [NOTE: The Preamble section of the security rule notes that the rapid advances in technology in the area of encryption makes it impractical and inappropriate to name a specific technology. Some older encryption algorithms with small key sizes can easily be broken in today's technically advanced society Each covered entity should carefully evaluate these technological advances so as to reap the benefits of more mature solutions.]

## Integrity Controls

Integrity is the process protecting data from improper alteration or destruction during transit. Digital Signatures and Message Digest (One-way Hash) both allow for the assurance that electronic protected health information is truly from the sending entity and has not been modified.

Digital Signatures use public/private keys that validate the authenticity of an entity. The originator of the transmission digitally signs the data using its private key, and then the recipient of the data uses the originators public key to ensure the original person sent the data.

One-way Hashing uses a function to create a message digest. This function can be used to ensure that the data was not changed during transit.

# POLICY & PROCEDURE

<b>Practice:</b> Organization Name	<b>Effective Date:</b> April 14, 2005
<b>Title:</b> Electronic Transmission Security of PHI	<b>Date Revised:</b> April 14, 2005
<b>Policy Number:</b> 2245	<b>Reference:</b> 45 CFR § 164.312(e)(1) + (2)

Consider related technical policies: See PERSON OR ENTITY AUTHENTICATION, EMAIL AND PROTECTED HEALTH INFORMATION and FACSIMILE MACHINES AND PROTECTED HEALTH INFORMATION.

3. The chair of the committee will assure that all decisions related to the solution (s) chosen are well documented and retained in accordance with [ENTITY] retention policy. This includes documentation supporting "further assessment" activities in support of "Addressable" Implementation Specifications. [Note: The various draft versions of each policy may be utilized to support this documentation process. Consider adding a "Note Section" at the bottom and be sure to archive all draft/working versions of the templates.]
4. Once a process and/or technical solution is chosen, the Security Official will work with the committee to assure the various related implementation subtasks are appropriately assigned allowing for a realistic implementation process.
5. The Security Official will additionally assure that any and all related policies and procedures will be updated, including training materials.
6. To the extent that workforce functions are affected by the chosen solution, the training department will work with managers to coordinate and assure that the solution is implemented and each affected member is trained.
7. The Security Official will assure that routine monitoring of this solution is carried out on a (daily, monthly, quarterly) basis in order to continually assess the effectiveness of [ENTITY]'s ability to balance the confidentiality of the protected health information with its integrity and availability.

**REFERENCE:** 45 CFR § 164.312(e)(1) + (2)

See also: E-MAIL AND PROTECTED HEALTH INFORMATION  
FACSIMILE MACHINES AND PROTECTED HEALTH INFORMATION