Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Transmission Security*

HIPAA Regulation:

• *Transmission security*	§164.312(e)(1)	addressable
• *Integrity controls*	§164.312(e)(1)	addressable
• *Encryption*	§164.312(e)(1)	addressable

Policy Purpose:

The purpose of this policy is to guard against unauthorized access to, or modification of, electronic protected health information (EPHI) that is being transmitted over an electronic communications network. When EPHI is transmitted from one point to another, it shall be protected in a manner commensurate with the associated risk.

Policy Description:

Encryption

Proven, standard algorithms shall be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose.

Encryption Required

1. No EPHI shall be sent outside the **Saratoga Bridges** (Wan) Network unless it is encrypted. This includes all email and email attachments sent over the Internet.
2. When accessing a secure network an encryption communication method, such as a Virtual Private Network (VPN), shall be used.

Encryption Optional

1. When using a private circuit (point to point) to transmit EPHI, such as authorized transmission of EPHI within the **Saratoga Bridges** WAN, no encryption is required. Or within the Saratoga Bridges internal network.
2. Dialup connections directly into secure networks are considered to be secure connections for EPHI and no encryption is required.

EPHI Transmissions Using Wireless LANs

1. The transmission of EPHI over a wireless network is permitted if both of the following conditions are met:
   a) The connection through the wireless network utilizes an authentication mechanism to ensure that wireless devices connecting to the network are authorized

   b) The connection through the wireless network utilizes an encryption mechanism for all transmissions over the network
2. If transmitting EPHI over a wireless network that is not utilizing an authentication and encryption mechanism, the EPHI shall be encrypted before transmission.

Perimeter Security

1. Any external connection to the **Saratoga Bridges** WAN shall come through the perimeter security's managed point of entry.
2. If determined safe, outbound services shall be initiated for internal addresses to external addresses.
3. Inbound services shall be negotiated on a case by case basis.
4. All workforce members connecting to the **Saratoga Bridges** WAN shall sign the **Saratoga Bridges** IT Security Policy before connectivity is established.

Firewall Controls

1. Networks containing systems and applications with EPHI shall implement perimeter security and access control with a firewall.
2. Firewalls shall be configured to support the following minimum requirements:
   a) Limit network access to only authorized workforce members and entities
   b) Limit network access to only legitimate or established connections
   c) Console and other management ports shall be appropriately secured or disabled
3. The configuration of firewalls used to protect networks containing EPHI based systems and applications shall be IT department for review and approval.

Policy Responsibilities:

Workforce Member Responsibilities

All workforce members that transmit EPHI outside the **Saratoga Bridges** WAN are responsible for ensuring the information is safeguarded by using encryption when using the Internet or a wireless connection.

IT Support Responsibilities

The **Saratoga Bridges** IT Department is responsible for the perimeter security architecture, its resources, its periodic auditing, and testing.