Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Virtual Private Network (VPN)*

Policy Purpose:

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the **Saratoga Bridges** corporate network.

This policy applies to all **Saratoga Bridges** employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the **Saratoga Bridges** network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

Policy Description / Responsibilities:

Approved Saratoga Bridges employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the ***Remote Access Policy***.

In addition:

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to **Saratoga Bridges** internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by **Saratoga Bridges** network operational groups.
6. All computers connected to **Saratoga Bridges** internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from **Saratoga Bridges** network after a period of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not **Saratoga Bridges** owned equipment must configure the equipment to comply with **Saratoga Bridges** VPN and Network policies.
10. Only IT Department-approved VPN clients may be used.

11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of **Saratoga Bridges** network, and as such are subject to the same rules and regulations that apply to **Saratoga Bridges**-owned equipment, i.e., their machines must be configured to comply with the IT Department's Security Policies.