Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Wireless Communication*

Policy Purpose:

This policy prohibits access to **Saratoga Bridges** networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the IT Department are approved for connectivity to **Saratoga Bridges** networks.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of **Saratoga Bridges** internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to **Saratoga Bridges** networks do not fall under the purview of this policy.

Policy Description / Responsibilities:

Register Access Points and Cards
All wireless Access Points/Base Stations connected to the corporate network must be registered and approved by IT Department. These Access Points/base stations are subject to periodic penetration tests and audits. All wireless Network Interface cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with IT Department.

Approved Technology
All wireless LAN access must use corporate-approved vendor products and security configurations.

VPN Encryption and Authentication
To comply with this policy, wireless implementations must maintain point to point hardware encryption of appropriate length.

Setting the SSID
The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.