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

Policy Purpose:

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of **Saratoga Bridges**.

All routers and switches connected to **Saratoga Bridges** production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the ***Internet DMZ Equipment Policy***.

Policy Description / Responsibilities:

Every router must meet the following configuration standards:

1. The enable password on the router must be kept in a secure encrypted form if possible. The router must have the enable password set to the current production router password from the router's support organization.
2. Disallow the following:
    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router
3. Use corporate standardized SNMP community strings.
4. Access rules are to be added as business needs arise.
5. The router must be included in the corporate enterprise management system with a designated point of contact.
6. Each router must have the following statement posted in clear view:
   "Saratoga Bridges Device. Unauthorized Access Prohibited. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."