Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Risk Analysis and Management*

HIPAA Regulation:

• *Perform a periodic technical and non-technical evaluation*	§164.308(a)(8)	required
• *Security management process*	§164.308(a)(1)	required
• *Risk analysis*	§164.308(a)(1)	required
• *Risk management*	§164.308(a)(1)	required
• *Information System Activity Review*	§164.308(a)(1)	required

Policy Purpose:

The purpose of this policy is to establish periodic evaluations of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (EPHI) held by **Saratoga Bridges** and to manage the security of the EPHI by identifying, controlling, and mitigating risks.

Policy Description:

Saratoga Bridges shall perform risk analysis and management through periodic assessments and implementation of controls to mitigate risks.

Risk Analysis

In order to conduct an accurate and thorough assessment of potential risks and vulnerabilities to the EPHI held by **Saratoga Bridges**, the following activities shall be conducted and documented:

1. Periodic program assessments including a security review of facility access controls, protection of network server closets, workstations, portable devices, and document destruction capabilities.
2. Assessments of new or existing information system applications that contain, or are used to protect EPHI.
3. Assessments of modifications to existing facilities or development of new facilities that maintain or house EPHI.
4. Assessments of new programs, departments, or changes in the mode or manner of service delivery involving EPHI.

Risk Management

Security measures and controls, sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, shall be implemented:

1. Workforce security training and awareness reminders
2. Access controls, authorization and validation procedures
3. Detection and activity reviews
4. Applications and data criticality analysis
5. IT systems change management
6. Incident reporting and response procedures
7. Sanctions for non-compliance
8. Contingency, Data Backup, and Disaster Recovery Planning

IT Change Management

The risk management process shall include change controls for all alterations that occur in the information systems that support, contain, or protect EPHI. These alterations include but are not limited to:

1. Installation, update, or removal of network services and components
2. Operating systems upgrades
3. Installation, update, or removal of applications, software, and database servers

IT change management notification and implementation shall follow the policies and procedures as documented by IT support.

Policy Responsibilities:

IT Support Responsibilities

1. Inform the Office of Compliance of the planned installation, update, or removal of any applications containing EPHI in a HIPAA covered component.