Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Audit Controls*

HIPAA Regulation:

• *Log-in monitoring*	§164.308(a)(5)	addressable
• *Information system activity review*	§164.308(a)(1)	required
• *Audit controls*	§164.312(b)	required

Policy Purpose:

The purpose of this policy is to establish the standard of authority to conduct security monitoring and enforce audit controls on computing resources used by HIPAA covered components.

Policy Description:

Saratoga Bridges has the requirement to monitor system access and activity of all HIPAA covered component workforce members.

Log-in Monitoring

To ensure that access to servers, workstations, and other computer systems containing electronic protected health information (EPHI) is appropriately secured, the following log-in monitoring measures shall be implemented:

1. A mechanism to record all failed log-in attempts on network systems containing EPHI when the technology is capable of auditing.
2. To the extent that technology allows, a means to disable any User ID that has more than six consecutive failed log-in attempts within a 30-minute period.
3. A review of log-in activity reports and logs when required to identify any patterns of suspicious activity, such as continuous failed log-in attempts.

Information System Activity Review

Information system activity reviews and audits may be conducted to:

1. Ensure integrity, confidentiality, and availability of information and resources.
2. Investigate possible security incidents to ensure compliance with Saratoga Bridges Information Technology (IT) and security policies.
3. Monitor user or system activity as required.
4. Verify that software patching is maintained per IS Department practices.
5. Verify that virus protection is current.

Information System Audit Controls

To ensure that activity for all computer systems accessing EPHI is appropriately monitored and reviewed, these requirements shall be met:

1. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
2. Each fiscal quarter, at a minimum, IT support shall review audit logs, activity reports, or other mechanisms for indications of improper use.
3. Indications of improper use shall be reported to management for investigation and follow up.
4. Audit logs of access to networks and applications with EPHI shall be archived and protected from unauthorized access, modification, and deletion.

Policy Responsibilities:

IT Support Responsibilities

1. Implement and manage the log-in monitoring and audit controls through activity reports on systems containing EPHI to comply with the HIPAA Security Rule.
2. Report all suspicious log-in or system activity to management for investigation and follow-up.

Supervisor and Manager Responsibilities

1. Work with IT support to ensure that user and system activity reports provide sufficient information to determine if improper use of EPHI has occurred.
2. Work with IT support to investigate reports of potential misuse of log-in accounts or access to EPHI by their workforce.