Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Security Incident Reporting, Risk Assessment, and Response*

HIPAA Regulation:

• *Security incident procedures*	§164.308(a)(6)	required
• *Reporting and response*	§164.308(a)(6)	required

Policy Purpose:

The purpose of this policy is to formalize the response to, and reporting of, security incidents. This includes identification and response to suspected or known security incidents, the mitigation of the harmful effects of known or suspected security incidents to the extent possible, and the documentation of security incidents and their outcomes.

Policy Description:

Saratoga Bridges shall identify, document, and respond to unauthorized use of the systems that contain electronic protected health information (EPHI).

Incident Reporting
All security incidents, threats to, or violations of, the confidentiality, integrity, or availability of electronic protected health information (EPHI) shall be reported and responded to promptly.

Incidents that shall be reported include, but are not limited to:

1. EPHI data loss due to disaster, failure, error, or theft
2. Loss of any electronic media that contains EPHI
3. Loss of the integrity of EPHI
4. Virus, worm, or other malicious code attacks
5. Persistent network or system intrusion attempts from a particular entity
6. Unauthorized access to EPHI, or an EPHI-based system or network
7. Facility incidents, including but not limited to:
    - Unauthorized person found in a HIPAA covered component's facility
    - Facility break-in
    - Lost or stolen key, badge, or cardkey

Workforce members shall notify their manager or supervisor of any suspected or confirmed security incident. The manager or supervisor shall report the incident to the Information Technology (IT) Service Desk at 587-0723 Ext: 1333 The IT Service Desk will evaluate the situation to determine if it is a potential security incident, and initiate the response process as required by the type of incident.

If a facility incident occurs, the manager or supervisor shall immediately report the incident to their facility manager, and to the IT Service Desk if appropriate.

If the security involves any breach of EPHI, the manager or supervisor shall notify the Compliance Officer and Security Officer, in addition to notifying the IT Service Desk.

Incident Response and Resolution

The IT Service Desk shall receive and record basic information on the incident and forward the information to the appropriate staff for response to that type of incident, i.e., a computer virus incident to the IT staff that provides anti-virus support.

The IT staff receiving the security incident service request shall perform their assigned responsibilities to respond to and/or mitigate any incident consequences. The IT staff responsible for determining if a possible EPHI breach has resulted from the incident shall notify the Compliance Officer.

The Compliance Officer and Security Officer shall evaluate the incident to determine if a breach of EPHI occurred. If it is determined that a breach has occurred, the Compliance Officer and Security Officer shall perform and document risk assessments on such breaches. The Compliance Officer and Security Officer shall then coordinate any mandated notification processes.

Incident Logging

All HIPAA security related incidents and their outcomes will be logged by the IT Service Desk and documented by the assigned IT support staff.

Policy Responsibilities:

Workforce Member Responsibilities

Workforce members are responsible to promptly report any potential security related incident to their manager or supervisor, or directly to the IT Service Desk at 587-0723 Ext: 1333

Supervisor and Manager Responsibilities

1. Ensure that the IT Service Desk and the Compliance Officer and Security Officer are notified of any security incident.
2. Ensure that the facility manager is notified of any facility related incident as described in the **Incident Reporting** section above.

Manager/Supervisor Responsibilities

Ensure that facility-related security incidents are reported and responded to as directed by the HIPAA covered component's policies and procedures.

IT Service Desk Responsibilities

1. Log all reported security incidents for HIPAA covered components.
2. Perform duties to investigate, respond to, and/or mitigate any incident consequences.
3. Notify Compliance Officer and Security Officer when a breach of EPHI is suspected or may have occurred.
4. Provide a report to Compliance Officer and Security Officer quarterly, to be retained for six years.

Compliance Officer and Security Officer Responsibilities

1. Determine if the incident requires further investigation and if it is a breach of EPHI. Working with the affected departments, determine if corrective actions should be implemented.
2. Document EPHI breach investigations and any corrective actions.
3. Maintain all documentation on EPHI breaches for a minimum of six years.