Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Facility Access Controls*

HIPAA Regulation:

• *Facility security plan*	§164.310(a)(1)	addressable
• *Facility access controls*	§164.310(a)(1)	addressable
• *Access control and validation procedures*	§164.310(a)(1)	addressable
• *Maintenance records*	§164.310(a)(1)	addressable
• *Contingency operations*	§164.310(a)(1)	addressable

Policy Purpose:

The purpose of this policy is to establish protocols for securing facilities that contain electronic protected health information (EPHI).

Policy Description:

Saratoga Bridges shall reasonably safeguard EPHI from any intentional or unintentional use or disclosure. **Saratoga Bridges** shall protect its facilities where EPHI can be accessed.

Facility Security Plan

Saratoga Bridges shall use reasonable safeguards in the facilities of its HIPAA covered components and the equipment therein from unauthorized physical access, tampering, and theft.

There shall be periodic audits of HIPAA covered components to ensure EPHI safeguards are continuously being maintained.

When designing a new building and remodeling existing sites, facility managers and/or designees shall work with the Compliance Officer to ensure the facility plan components below are compliant with federal HIPAA regulations.

The following shall be implemented for all sites that access EPHI:

1. **Visitor Access Control**: Each facility shall implement procedures that govern visitor access controls. These procedures may vary depending on the facility structure, the type of visitors, and where the EPHI is accessible.

2. **Metal/Hard Keys**: Facilities that use metal/hard keys shall develop and document protocols to govern situations when keys are lost or a workforce member leaves without returning the key. In addition, the facility shall have:
    a) Clearances based on programmatic need, special mandated security requirements, and workforce member security; and
    b) A mechanism to track which workforce members are provided access.
3. **Network Closet(s):** All core network closets shall be secured (where possible), whenever the closet is unoccupied or not in use.
4. **Server Room(s):** Every server room shall be locked whenever the room is unoccupied or not in use, or shall be enclosed in a locked equipment cage. Only authorized personnel are granted access to server rooms.
5. **Doors:** Each facility will develop, document and implement procedures for dealing with non-public doors and securing/monitoring access to the facility. It is each workforce member's responsibility to make sure that the applicable door that is being entered or exited is completely shut before leaving the door. If a door's closing or locking mechanism is not working, it is every worker's responsibility to notify the facility manager or designee for that facility.

Policy Responsibilities:

Supervisor and Manager Responsibilities

1. Take appropriate corrective action if any workforce member knowingly violates the facility security plan and its procedures.
2. Authorize clearances that are appropriate to the duties of each workforce member.
3. Notify the manager or designee within one business day when a user no longer requires access to the facility.
4. Verify that each workforce member surrenders her/his card or key upon leaving employment.
5. Work with facility manager to ensure a log is kept of all access into network closets.

Workforce Member Responsibilities

1. Display their access/security card or employee badge to demonstrate their authorization to access restricted areas.
2. Do not allow other persons to enter the facility by "tailgating" (entering the facility by walking behind an authorized person through a door without valid identification).
3. Do not share access hard keys, alarm codes or keypad codes to enter the facility or areas where there is EPHI.
4. Immediately report lost or stolen ID cards, metal keys, or keypad-cipher lock combinations.
5. Surrender ID cards and/or hard key(s) upon leaving employment.

Facility Manager Responsibilities

1. Request and track maintenance repairs.
2. Establish and maintain a mechanism for accessing the facility in an emergency.
3. Track who has access to the facility.
4. Change metal locks when a key is lost or unaccounted for.
5. Change combination keypads/cipher locks every three months.

Corporate Compliance and HIPAA Compliance Officer Responsibilities

1. Work with managers to ensure that all **Saratoga Bridges** facilities comply with the HIPAA Security Rule for access controls.
2. Conduct periodic audits of HIPAA covered components to ensure their facilities are secure and the requirements of this policy are enforced.