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

HIPAA Regulation:

• *Access control and validation*	§164.312(a)(1)	required
• *Workstation use*	§164.310(b)	required
• *Workstation security*	§164.310(c)	required
• *Automatic log off*	§164.312(a)(1)	addressable

Policy Purpose:

The purpose of this policy is to establish rules for securing workstations that access electronic protected health information (EPHI). Since EPHI can be portable, this policy requires workforce members to protect EPHI at **Saratoga Bridges** worksites and all other locations.

Policy Description:

Saratoga Bridges shall implement safeguards to prevent unauthorized access to EPHI through workstations and to protect EPHI from any intentional or unintentional use or disclosure.

Workstation Security Controls
All workstations used by workforce members with access to EPHI shall be set to automatically lock the computer when it is left unattended, requiring the user to enter a password to unlock the workstation. The standard setting for the computer to lock after a period of inactivity is not to exceed 10 minutes.

Workforce members shall manually lock their workstation computer using the Ctrl-Alt-Delete key combination when the computer is left unattended for any period of time.

Workforce members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and access on computer screens. At each site, every effort shall be made to ensure that confidential information on computer screens is not visible to unauthorized persons.

Workforce members who work from home or other non-office sites shall follow the above workstation security controls to safeguard EPHI access or viewing by any unauthorized individual.

Workforce members shall protect printed versions of EPHI that have been transmitted via fax or multi-use machines by promptly removing documents from shared devices.

Whenever possible, confidential documents are to be placed in locked cabinets or drawers when left unattended.

Policy Responsibilities:

Supervisor and Manager Responsibilities

1. Control workforce member access to EPHI as per the ***User Access Management Policy***.
2. Take appropriate corrective action if any workforce member knowingly violates the security of workstation use.
3. Ensure that the automatic lock is functioning on all workstations.
4. Ensure that all workforce members are locking their workstations when they are left unattended.
5. Ensure that all confidential information is not viewable by unauthorized persons at workstations in offices under their management.

Workforce Member Responsibilities

1. Lock their computer when it is left unattended for any period of time.
2. Do not change or disable the automatic inability lock on their workstation.
3. Ensure that all confidential information in their workstation is not viewable or accessible by unauthorized persons.
4. When working from home or other non-office work sites, protect EPHI from unauthorized access or viewing.

IT Support Responsibilities

1. When installing new workstations, set the computer to automatically lock after the recommended period of inactivity, which is not to exceed 10 minutes.