Policy and Procedure: HIPAA/HITECH Compliance
Topic: *User Access Management*

HIPAA Regulation:

• *Workforce security*	§164.308(a)(3)	addressable
• *Workforce Authorization and/or supervision*	§164.308(a)(3)	addressable
• *Workforce clearance procedure*	§164.308(a)(3)	addressable
• *Workforce Termination procedure*	§164.308(a)(3)	addressable
• *Information access management*	§164.308(a)(4)	addressable
• *Access authorization*	§164.308(a)(4)	addressable
• *Access establishment and modification*	§164.308(a)(4)	addressable
• *Access control*	§164.312(a)(1)	required
• *Integrity*	§164.312(c)(1)	addressable
• *Emergency access procedure*	§164.312(a)(1)	addressable

Policy Purpose:

The purpose of this policy is to establish rules for authorizing access to the computing network, applications, workstations, and to areas where electronic protected health information (EPHI) is accessible. The HIPAA covered components shall ensure that only workforce members who require access to EPHI for work related activities shall be granted access and when work activities no longer require access, authorization shall be terminated.

In section §160.103 of the HIPAA Privacy Rule, the "workforce" is defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."

Policy Description:

Management and Access Control

Only the workforce member's manager or an appropriate designee can authorize access to the **Saratoga Bridges** information systems.

Access to the information system or application may be revoked or suspended, consistent with **Saratoga Bridges** policies and practice, if there is evidence that an individual is misusing information or resources. Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measures.

Minimum Necessary Access

Saratoga Bridges shall ensure that only workforce members who require access to Electronic Protected Health Information (EPHI) are granted access.

Each manager or supervisor is responsible for ensuring that the access to EPHI granted to the workforce member is the minimum necessary access required for each work role and responsibilities.

If the workforce member no longer requires access, it is the responsibility of the manager or appropriate designee to complete the necessary process to terminate access.

Granting Access to EPHI

Screen Workforce Members Prior to Access

The manager or designee shall ensure that information access is granted only after first verifying that the access of a workforce member to EPHI is appropriate.

Sign Security Acknowledgement

Prior to being issued a User ID or logon account to access any EPHI, each workforce member shall sign the **Saratoga Bridges** Access Policy before access is granted to the network or any application that contains EPHI, and thereafter shall comply with all **Saratoga Bridges** security policies and procedures.

Security Awareness Prior to Getting Access

Before access is granted to any of the various systems or applications that contain EPHI, the manager or appropriate designee shall ensure that workforce members are trained to a minimum standard including:

1. Proper uses and disclosures of the EPHI stored in the systems or application
2. How to properly log on and log off the systems or application
3. Protocols for correcting user errors
4. Instructions on contacting a designated person or help desk when EPHI may have been altered or destroyed in error
5. Reporting a potential or actual security breach

Management/Supervisor Approval

Implement the following policies and procedures:

1. User IDs or logon accounts can only be assigned with management approval or by an appropriate designee.
2. Managers or their designees are responsible for requesting the appropriate level of access for staff to perform their job function.
3. All requests regarding user IDs or computer system access for workforce members are to be communicated to the system administrator. All requests shall be made in writing (which may be in an electronic format).
4. System administrators are required to process only those requests that have been authorized by managers or their appropriate designees.

5. A written or electronic record of the authorized request is to be retained by the system administrator for a period of time the approved user has access, plus a minimum of one year.

Granting Access in an Emergency

Management has the authority to grant emergency access for workforce members who have not completed the normal HIPAA access requirements if:

1. Management declares an emergency or is responding to a natural disaster that makes client information security secondary to personnel safety.
2. Management determines that granting immediate access is in the best interest of the client.
3. If emergency access is granted, the manager shall review the impact of emergency access and document the event within 24 hours of it being granted.
4. After the emergency event is over, the user access shall be removed or the workforce member shall complete the normal requirements for being granted access.

Termination or Suspension of Access

Department managers or their designated representatives are responsible for terminating a workforce member's access to EPHI in these circumstances:

1. If management has evidence or reason to believe the individual is using information systems or resources in a manner inconsistent with HIPAA Security Rule policies.
2. If the workforce member or management has reason to believe the user's password has been compromised.
3. If the workforce member resigns, is terminated, suspended, retires, or is away on unapproved leave.
4. If the workforce member's work role changes and system access is no longer justified.

If the workforce member is on a leave of absence and the user's system access will not be required for more than four weeks, management shall suspend the user's account until the workforce member returns from their leave of absence.

Modifications to Access

If a workforce member transfers to another department or changes their work role within the same department, the workforce member's new manager or supervisor is responsible for evaluating the member's current access and for requesting new access to EPHI commensurate with the workforce member's new work role and responsibilities.

Ongoing Compliance for Access

In order to ensure that workforce members only have access to EPHI when it is required for their job function, the following actions shall be implemented:

1. Every new user ID or logon account that has not been used after 30 consecutive calendar days since creation shall be investigated to determine if the workforce member still requires access to the EPHI.
2. At least every six months, Information Technology (IT) teams are required to send managers or appropriate designees:
    - A list of all workforce members for all applications
    - A list of all workforce members and their access rights for all shared folders that contain EPHI
    - A list of all workforce members approved for access to Virtual Private Network (VPN)
3. The managers or their designees shall then notify IT support of any workforce members who no longer require access.

Policy Responsibilities:

Manager and Supervisor Responsibilities

1. Ensure that the access to EPHI granted to each of their workforce members is the minimum necessary access required for each such workforce member's work role and responsibilities.
2. In order to protect the security of the file server from malicious intent or unauthorized use by non-employees, each department manager is responsible to report employee termination (voluntary and non-voluntary), employee suspension, or employees expected to be on leave for more than four weeks (medical, workers comp, etc.) to the IT Department within 24 hours. The IT Department will disable computer access upon notification.
3. Request termination of access if the workforce member no longer requires access.
4. Validate new User IDs or logon accounts that are not used within 30 days of creation and provide IT with that information.
5. Review semi-annual user and folder access reports and the VPN access reports prepared by IT support and verify to determine if the workforce members still require access to EPHI.
6. Ensure that members of the workforce have signed the IT security agreement and are properly trained before approving access to EPHI.
7. Follow the appropriate security procedures when granting emergency access with support from IT where required.

IT Support Responsibilities

1. Immediately upon written notification, remove or modify a workforce member's access to EPHI.
2. Provide management with a report that identifies new User IDs or logon accounts not used within 30 days of creation.
3. Provide management with a semi-annual report documenting workers with access to EPHI, and requesting verification that access is still required to fulfill the worker's job functions.
4. When required, support management with the appropriate security procedures for granting emergency access.

Workforce Member Responsibilities

Each user of a system or application that contains EPHI shall:

1. Read and sign the **Saratoga Bridges** Electronic Access Policy and the **Saratoga Bridges** HIPAA Privacy and Security Policies & Procedures Acknowledgement.
2. Follow all Information Security policies and requirements.
3. Complete HIPAA Privacy and Security training.
4. Immediately report all security incidents to their supervisor or other appropriate manner consistent with hospital policy.
5. Any employee who has a user account to access computer resources must take necessary precautions to keep confidential the password associated with that user account. Employees who feel that other individuals have knowledge of their password must report this to the IT Department so that the password can be changed.