Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Authentication and Password Management*

HIPAA Regulation:

• *Mechanism to authenticate electronic protected health information*	§164.312(c)(1)	addressable
• *Person or entity authentication*	§164.312(d)	required
• *Password management*	§164.308(a)(5)	addressable
• *Unique user identification*	§164.312(a)(1)	required

Policy Purpose:

The purpose of this policy is to ensure that workforce members select and secure strong passwords to authenticate their access to information systems containing electronic protected health information (EPHI).

Policy Description:

Information systems used to access EPHI shall uniquely identify and authenticate workforce members. When possible, all systems will meet the following minimum guidelines. Systems that are unable to meet the following guidelines will be noted in exceptions and upgraded when possible.

The password file on the authenticating server shall be adequately protected and not stored in plaintext (unencrypted).

1. Automatic password expiration at User ID creation and password reset.
2. Automatic password expiration every 120 days.
3. A minimum password length of 8 characters.
4. A minimum of five passwords are retained in the system that cannot be reused with a User ID.

User ID and Password Management

All workforce members are assigned a unique User ID to access the Saratoga Bridges network and are responsible for creating and maintaining the confidentiality of the password associated with their unique User ID.

Supervisors and managers are required to ensure that the workforce under their supervision understands the user responsibilities for securely managing confidential passwords.

Upon receipt of a User ID, the workforce member assigned the User ID is required to change the password provided by the administrator to a password that only he or she knows. Strong passwords shall be created in order to secure access to EPHI.

Workforce members who suspect that their password has become known by another person shall change their password immediately. Work members shall not share with or reveal their password to anyone, including their supervisor, manager, or IT support staff.

All privileged system-level passwords (e.g., root enable, application administration accounts, etc.) shall be changed, at a minimum, each fiscal quarter.

All passwords are to be treated as sensitive, confidential Saratoga Bridges information. If the workforce member's manager or supervisor requires emergency access to a worker's email or individual network drive, refer to **Granting Access in an Emergency** under the ***User Access Management Policy***.

Strong Password Guidelines

Select strong passwords that have the following characteristics:

1. The password contains at least 8 characters.
2. The password contains both upper and lower case characters.
3. The password contains at least one number or special character (such as @, #, $, %).
4. The password is not so hard to remember that you have to write it down but it should remain difficult for others to guess.
5. Avoid using dictionary words.

Policy Responsibilities:

Manager and Supervisor Responsibilities

1. Reinforce secure password use by workforce members.
2. If access to another workforce member's account is required, follow the emergency access procedures in **Granting Access in an Emergency** under the ***User Access Management Policy*.**

IT Support Responsibilities

1. System administrators shall verify the identity and the authority of the workforce member or an authorized requester, such as the member’s manager or supervisor, before providing the password for a new User ID.
2. System administrators shall verify the identity and the authority of the workforce member requesting a password reset.
3. System administrators shall verify the identity and the authority of an authorized requester, such as the member’s manager or supervisor, to request a password reset for another workforce member.

Workforce Member Responsibilities

1. Create and securely manage strong passwords for access to systems containing EPHI.
2. Follow the password protection requirements to protect the confidentiality of their passwords to ensure security of EPHI:
   - Passwords shall not be shared with or revealed to anyone, including their supervisor, manager, or IT support staff.
   - Passwords shall never be revealed on questionnaires or security forms.
   - Passwords shall be memorized, not written down.
   - The password used to access **Saratoga Bridges** network shall not be used anywhere else.
   - The password shall be changed immediately if the workforce member suspects it has become known by another person.