



Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Policy Documentation*

HIPAA Regulation:

• <i>Policies and procedures</i>	<u>§164.316(a)</u>	required
• <i>Documentation</i>	<u>§164.316(b)(1)</u>	required
• <i>Time limit</i>	<u>§164.316(b)(1)</u>	required
• <i>Availability</i>	<u>§164.316(b)(1)</u>	required
• <i>Updates</i>	<u>§164.316(b)(1)</u>	required

Policy Purpose:

The purpose of this policy is to establish the process by which **Saratoga Bridges** HIPAA Security Rule Policies and Procedures are created and maintained in accordance with federal regulations.

Policy Description:

Saratoga Bridges is required to have policies and procedures for compliance with the HIPAA Security Rule. All policies will be updated annually or at any significant infrastructure change.

Policies and Procedures

1. New or revised HIPAA Security Rule Policies and Procedures as required due to:
 - a. Changes in business practices or the Information Technology (IT) environment of the HIPAA covered components
 - b. Mandated federal law enacted by Congress
 - c. Risk analysis determines new or increased vulnerability to security threat
2. All policies and procedures implemented to comply with the HIPAA Security rule shall be made available to the HIPAA covered component workforce.
3. All actions, activities, or assessments required by the HIPAA Security Policies and Procedures shall be documented. The documentation shall provide sufficient detail to communicate the implemented security measures and to facilitate periodic evaluations by the HIPAA covered components or as requested by the Security Officer.
4. In accordance with 45 C.F.R. § 164.316, documentation shall be retained for a minimum of six (6) years from the time of its creation or the date it was last in effect, whichever is later.



Policy Responsibilities:

Compliance Responsibilities

1. Draft new or updated HIPAA Security Rule Policies and Procedures as indicated in the **Policies and Procedures** section above.
2. Communicate the approved new or revised policy to the workforce of the HIPAA covered components, and update training and related materials as needed.
3. Maintain and make available to the workforce the HIPAA Security Rule Policies and Procedures in electronic form.

Chief Information Security Officer/ Security Officer Responsibilities

Provide final approval of the **Saratoga Bridges** HIPAA Security Policies and Procedures.