Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Breach Notification and Risk Assessment Actions and Response*

HIPAA Regulation:

• *Policy and Procedures*	§164.402-414	required
• *Reporting and response*	§164.308(a)(6)	required

Policy Purpose:

The purpose of this policy is to formalize the response to, and reporting of, Protected Health Information (PHI), Electronic Protected Health Information (EPHI), and Personally Identifiable Information (PII) data security or privacy breach or disclosure incidents. This includes identification and response to suspected or known privacy and security incidents, the mitigation of the harmful effects of known or suspected incidents to the extent possible, and the documentation of incidents and their outcomes.

Policy Description:

Saratoga Bridges will respond to all impermissible uses or disclosures of protected health information and it will be presumed that a breach has occurred unless the **Saratoga Bridges** or its business associate, as applicable, demonstrates through the appropriate risk assessment process, that there is a low probability that the protected health information has been compromised. All disclosure, impermissible uses and breach incidents of electronic and hardcopy protected health information shall be reported and responded to promptly.

Workforce Member Responsibilities

Workforce members shall immediately notify their manager or supervisor of any suspected or confirmed breach or disclosure incident. The manager or supervisor shall report the incident to the Compliance Officer, Privacy Officer, and Security Officer at the corporate compliance website as defined in staff training, e-mail hipaa@saratogabridges.org, contact the security office or privacy officer directly at their extension, or call the corporate compliance hotline at 518-587-6824. The Compliance Officer, Privacy Officer, and Security Officer will, in concert together, evaluate the situation to determine the appropriate response to the report disclosure or breach incident, and initiate the response process as required by the type of incident.

Impermissible Uses, Breach or Disclosures Risk Assessment

The Compliance Officer, Privacy Officer, and Security Officer will WITHOUT UNREASONABLE DELAY:

1. Perform and document a risk assessment based on the disclosure/breach identified: the process to be followed is – based on the current rule:
    a. Instead of assessing the risk of harm to the individual, **Saratoga Bridges** and business associates must assess the probability that the protected health information has been compromised based on a risk assessment that considers at least the following factors:
        i. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (remember to include in the review a "sensitivity rating" - For example, with respect to financial information, this includes credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud – and if this is the case, then other laws may come into play);
        ii. The unauthorized person who used the protected health information or to whom the disclosure was made;
        iii. Whether the protected health information was actually acquired or viewed; and
        iv. The extent to which the risk to the protected health information has been mitigated.

Impermissible Uses, Breach or Disclosures Response and Resolution

Saratoga Bridges, following a breach or suspected breach of unsecured protected health information or PII, shall:

1. Provide notice of a breach to prominent media outlets serving a State or jurisdiction, following the discovery of a breach if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. This notice is in addition, not a substitute to, the required written notice, and shall be provided in the following form:
    a. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.
    b. If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

c. Substitute notice. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
d. In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.
e. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of **Saratoga Bridges**' web site, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a phone number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.
f. In any case deemed by **Saratoga Bridges'** to require urgency because of possible imminent misuse of unsecured protected health information, **Saratoga Bridges** may provide information to individuals by telephone or other means, as appropriate, in addition to written notice.
g. Inform prominent media outlets serving the State or jurisdiction.

2. Except as provided in §164.412, **Saratoga Bridges** shall provide the notification required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
3. The content of the notification required shall meet the requirements of §164.404(c) and shall include to the extent possible:
    a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    b. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
    c. Any steps the individual should take to protect themselves from potential harm resulting from the breach;
    d. A brief description of what **Saratoga Bridges** is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches;
    e. Contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an email address, website, or postal address; and
    f. The notification shall be written in plain language.

Saratoga Bridges shall, following the discovery (post risk assessment) of a breach of unsecured protected health information as provided in §164.404(a)(2):

1. Notify the Secretary of HHS.
2. For breaches of unsecured protected health information involving 500 or more individuals, **Saratoga Bridges** will provide the notification required in the manner specified on the HHS web site located at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.
3. For breaches of unsecured protected health information involving less than 500 individuals, **Saratoga Bridges** shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required for those breaches occurring during the preceding calendar year, in a manner specified on the HHS web site at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

Saratoga Bridges is required to notify all individuals when there has been or is reasonably believed to have been a unintended disclosure or compromise of the individual's private information (PII, PHR, PHI, etc.) in compliance with the applicable Information Security Breach and Notification Acts affecting **Saratoga Bridges** and this policy.

In addition:

1. **Saratoga Bridges** has in place the measures to monitor and detect the unauthorized access, disclosure, or compromise to private information stored within our premises or at third parties who store, transmit, or process PHR, PHI, ePHI, and PII on behalf of **Saratoga Bridges**.
2. **Saratoga Bridges** will attempt to assess any third party who stores, processes, or transmits PHI, PHR, or PII on **Saratoga Bridges'** behalf.
3. **Saratoga Bridges**, after consulting with the Information Security Officer to determine the scope of the breach and restoration measures, shall notify the individual when it has been determined that there has been, or is reasonably believed to have been a compromise of private information through unauthorized disclosure.
4. A compromise of private information shall mean the unauthorized acquisition of unencrypted computerized data with private information as identified as PHR, PHI, ePHI, and PII under the applicable laws and regulations.
5. In addition, if encrypted data is compromised along with the corresponding encryption key, the data shall be considered unencrypted and thus fall under the notification requirements.
6. It is understood that notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.

7. **The Privacy Officer** shall notify the Compliance Officer, and Security Officer as to the timing, content, and distribution of the notices and approximate number of affected persons.
8. **The Privacy Officer** shall notify the Attorney General, Consumer Protection Boards, and any other required agency or body whenever notification to an affected resident is necessary, as to the timing, breach identifications, content, and distribution of the notices and approximate number of affected persons.
9. Regardless of the method by which notice is provided, such notice shall include contact information for **Saratoga Bridges** making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.
10. This Policy also applies to information maintained on behalf of **Saratoga Bridges** by any third party.
11. When more than five hundred residents are to be notified at one time, **Saratoga Bridges** is required to notify the appropriate consumer reporting agencies, State Agencies, and Federal Agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals.
12. **Saratoga Bridges** will have in place a **Comprehensive Written Information Security Program (WISP).**

Impermissible Uses, Breach or Disclosures Response and Resolution Logging

Other than the above requirements for reporting to external agencies, all Impermissible Use, Breach, or Disclosure related incidents and their outcomes will be logged by the Compliance Officer, Privacy Officer, and Security Officer and all findings, outcomes, and communications documented. That documentation will be saved for at least seven years or as needed to meet any claims, legal challenges, or other compliance activities.

Each calendar year, the log will be reviewed and disclosures will be reported to the appropriate regulatory agency as required.

Policy Responsibilities:

1. The Compliance Officer, Privacy Officer, and Security Officer determine if the incident requires further investigation and if it is a breach of PHR, PHI, ePHI, and PII. Working with the affected departments, they shall determine if corrective actions should be implemented.
2. The Compliance Officer, Privacy Officer, and Security Officer are responsible for documentation of PHR, PHI, ePHI, and PII breach investigations and any corrective actions.
3. The Compliance Officer, Privacy Officer, and Security Officer are responsible for maintaining all documentation on PHR, PHI, ePHI, and PII breaches for a minimum of six years.