Saratoga Bridges Written Information Security Program

1.0 Policy Statement

The Saratoga Bridges Written Information Security Program (WISP) is intended as a set of comprehensive guidelines and policies designed to safeguard all sensitive data maintained at Bridges, and to comply with applicable laws and regulations on the protection of Personal Health Information (PHI, or ePHI), whether in electronic or other form, found on records and in systems owned by Saratoga Bridges.

2.0 Overview

In accordance with federal and state laws and regulations, Saratoga Bridges is required to take measures to safeguard PHI or ePHI (used interchangeably throughout the document) information, and to provide notice about security breaches of such information to affected individuals and appropriate federal and/or state agencies.

In addition, Saratoga Bridges is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who work or reside or attend programs at Saratoga Bridges. Saratoga Bridges has implemented a number of policies to protect such information, and the WISP should be read in conjunction with these policies that are cross-referenced at the end of this document.

3.0 Purpose

The purposes of this document are to:

- Establish a comprehensive information security program for Saratoga Bridges with policies designed to safeguard sensitive data that is maintained by Saratoga Bridges, in compliance with federal and state laws and regulations;
- Establish employee responsibilities in safeguarding data according to its classification level; and
- Establish administrative, technical and physical safeguards to ensure the security of sensitive data.

4.0 Scope

This Program applies to all Saratoga Bridges employees, whether full- or part-time, including staff, contract and temporary workers, hired consultants, interns, and volunteers, as well as to all other members of the Saratoga Bridges (hereafter referred to as the "Community"). The data covered by this Program includes any information stored, accessed or collected or for Saratoga

Bridges operations. The WISP is not intended to supersede any existing Saratoga Bridges policy that contains more specific requirements for safeguarding certain types of data, except in the case of Personal Information, as defined below. If such policy exists and is in conflict with the requirements of the WISP, the policy with more stringent protections takes precedence.

4.1 Definitions

Health information means any information, whether oral or recorded in any form or medium, that–

(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."

"*Individually identifiable health information* is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual."

Protected health information is defined in 45 CFR 160.103, where 'CFR' means 'Code of Federal Regulations', and, as defined, is referenced in Section 13400 of Subtitle D ('Privacy') of the HITECH Act.

"*Protected health information* means individually identifiable health information [defined above]:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) *Protected health information* excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer."

The HIPAA Privacy Rule covers protected health information in any medium while the HIPAA Security Rule covers electronic protected health information.

4.2 Data Classification

All data covered by this policy will be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level.

Confidential

Confidential data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a significant level of risk to Saratoga Bridges or the Community. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration or disclosure.

Confidential data includes any data that is protected by federal or state laws or regulations, including, but not limited to, data protected under the following privacy laws: Health Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA). Information protected by these laws includes, but is not limited to, PI, Protected Health Information (PHI).

Confidential data also includes other sensitive personal and institutional data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operations or reputation of Saratoga Bridges. This data includes, but is not limited to, donor information, research, intellectual property (proprietary research) Bridges financial and investment records, employee salary information, or information related to legal or disciplinary matters.

Internal Use Only

Internal Use Only data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a moderate level of risk to Saratoga Bridges. This data should be limited to access by individuals who are employed by or working for Saratoga Bridges in some capacity and who have legitimate reasons for accessing such data. Any non-public data that is not explicitly designated as Confidential should be treated as Internal Use Only data. A reasonable level of security should be applied to this classification to ensure the privacy and integrity of this data.

Public (or Unrestricted)

Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to Saratoga Bridges or members of the Saratoga Bridges community. Any data that is not classified as Confidential or Internal Use Only should be considered Public data.

5.0 Policy

5.1 Responsibilities

All data at Saratoga Bridges is assigned a data owner according to the constituency it represents. Data owners are responsible for approval of all requests for access to such data. The data owners for each constituency group are designated as follows:

- Official Health Records - (or his or her designee) serves as the data owner
- Staff data - (or his or her designee) serves as data owner

The Information Systems staff (IS/IT)serve as the data steward for all data stored centrally on Bridges servers and administrative systems, and are responsible for the security of such data. For distributed data stored on local machines the department head or their designee serves as the data steward, and (IS/IT) and the department share joint responsibility for securing the data.

Human Resources will inform (IS/IT) staff about an employee's change of status or termination as soon as is practicable but before an employee's departure date from Saratoga Bridges. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to Bridges data. IS/IT staff will terminate all of the employee's account access upon the employee's termination date from Saratoga Bridges, as specified by Human Resources.

Department heads will alert IS/IT at the conclusion of a contract for individuals that are not considered Bridges employees, who have electronic access, in order to terminate access to their Bridges accounts.

The Saratoga Bridges Information Security Officer (ISO), in collaboration with the Bridges Hipaa Committee on Data and Network Security, is in charge of maintaining, updating, and implementing this Program. The ISO can be contacted at hipaa@saratogabridges.org . Saratoga Bridges Director of Information Systems has overall responsibility for this Program.

All members of the Community are responsible for maintaining the privacy and integrity of all sensitive data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All members of the Community are required to access, store and maintain records containing sensitive data in compliance with this Program.

5.2 Identification and Assessment of Risks to Bridges Information

Saratoga Bridges recognizes that it has both internal and external risks to the privacy and integrity of Bridges information. These risks include, but are not limited to:

- Unauthorized access of Confidential data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of Confidential data by employees
- Unauthorized requests for Confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential data through third parties

Saratoga Bridges recognizes that this may not be a complete list of the risks associated with the protection of confidential data. Since technology growth is not static, new risks are created regularly. Accordingly, IS/IT will actively participate and monitor security resources and collaborate with other NYSARC agencies for identification of new risks.

Saratoga Bridges believes the current safeguards in place are reasonable and, in light of current risk assessments made by IT/IS, are sufficient to provide security and confidentiality to confidential data maintained by Saratoga Bridges. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

5.3 Policies for Safeguarding Confidential Data

To protect confidential data, the following policies and procedures have been developed that relate to protection, access, storage, transportation, and destruction of records, computer system safeguards, and training.

Access

- Only those employees or authorized third parties requiring access to confidential data in the regular course of their duties are granted access to confidential data, including both physical and electronic records.
- Computer and network access passwords are disabled upon termination of employment or relationship with Saratoga Bridges.
- Upon termination of employment or relationship with Saratoga Bridges, physical access to documents or other resources containing Confidential data is immediately prevented.

Storage

- Members of the Community will not store confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). In rare cases where it is necessary to transport confidential data electronically, the mobile device containing the data must be encrypted.
- To the extent possible, making sure that all confidential data is stored only on secure servers maintained by Saratoga Bridges or its authorized representatives and not on local machines, unsecure servers, or portable devices.
- Paper records containing confidential data must be kept in locked files or other secured areas when not in use.
- Electronic records containing confidential data must be stored on secure servers, and, when stored on authorized desktop computers, must be password protected.
- PHI must never be stored or shared using outside e-mail or cloud services such as Google Docs, or Microsoft SkyDrive unless a business associate agreement is in place with Saratoga Bridges prior to such usage.

Removing Records from Saratoga Bridges

- Members of the Community are strongly discouraged from removing records containing confidential data off Saratoga Bridges property. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing confidential data to be left unattended in any insecure location.
- When there is a legitimate need to provide records containing confidential data to a third party, electronic records shall be password-protected and/or encrypted, and paper records shall be marked confidential and securely sealed.

Destruction of Confidential Data

- Paper and electronic records containing confidential data must be destroyed in a manner that prevents recovery of the data in accordance with existing federal and state laws, and best practices.

Third-Party Vendor Agreements Concerning Protection of Confidential Data

Saratoga Bridges exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for Confidential Data provided by the Bridges to them. The primary budget holder for each department is responsible for identifying those third parties providing services to Saratoga Bridges that have access to Confidential Data. All relevant contracts with these third parties are reviewed and approved by Saratoga Bridges to ensure the contracts contain the necessary language regarding safeguarding Confidential Data. It is the responsibility of the primary budget holders to confirm that the third parties are required to maintain appropriate security measures to protect Confidential Data consistent with this Program and state/federal laws and regulations.

5.5 Computer system safeguards

The ISO monitors and assesses information safeguards on an ongoing basis to determine when enhancements are required. Saratoga Bridges has implemented the following to combat external risk and secure the College network and Confidential Data including PHI:

- Secure user authentication protocols
- Unique passwords are required for all user accounts; each employee receives an individual user account.
- Server accounts are locked after multiple unsuccessful password attempts.
- Computer access passwords are disabled upon an employee's termination.
- User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.
- Secure access control measures
- Access to specific files or databases containing PHI is limited to those employees who require such access in the normal course of their duties.
- Each such employee has been assigned a unique password to obtain access to any file or database that contains PHI needed by the employee in the course of his or her duties.
- Files containing PHI (or other Confidential Information) transmitted outside of the Saratoga Bridges network are to be encrypted.
- The ISO performs regular internal network security audits to all server and computer system logs to discover to the extent reasonably feasible possible electronic security

breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PHI.

- All Saratoga Bridges computers and servers are firewall protected and regularly monitored.
- Operating system patches and security updates are installed to all servers at least every 60 days.
- Antivirus and anti-malware software is installed and kept updated on all servers (where it is practicable—regardless of individual installation all external to internal traffic is scanned) and workstations. Virus definition updates are installed on a regular basis, and the entire system is tested and checked at least once per month.

5.5 Employee Training

All employees who access confidential data via external access or who otherwise have access to PHI are required to complete a yearly training on data security and their responsibilities related to this Program. Human Resources/the Training Department maintains records of all such training.

5.6 Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the ISO.

The ISO is charged with the identification of all data security incidents where the loss, theft, unauthorized access, or other exposure of sensitive Bridges data is suspected. The ISO reports any such incidents to the Director of Information Systems. When the ISO confirms an incident involving sensitive information, specifically a Hipaa Breech, the ISO will alert the Corporate Compliance Officer. The Corporate Compliance Officer will follow appropriate protocols and contact the necessary individuals to investigate and respond to the incident.

The ISO will document all breaches and subsequent responsive actions taken. All related documentation will be stored in the Finance Office.

For more information about incident response, including specific procedures for responding to a breach, see the Saratoga Bridges Incident Response Plan.

6.0 Enforcement

Any employee, contractor, or volunteer who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises data classified as Confidential or Internal Use Only without authorization, or who fails to comply with this Program in any other respect, will be subject to

disciplinary action, which may include termination in the case of employees and referral to state/federal authorities of warranted.

7.0 Effective date

This Written Information Security Program was implemented XXX. Saratoga Bridges will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.