Policy and Procedure: *HIPAA/HITECH Compliance*
Topic: *Safeguards for Confidentiality*

Policy Description:

It is the policy of **Saratoga Bridges** that all employees, volunteers, and contractors ensure confidentiality and privacy in regard to history, records, and discussions about individuals served. The very fact that an individual is served by this organization must be kept private or confidential; disclosures can be made only under specified conditions and with the appropriate authorization of the individual, the individual's personal representative, or an appropriate Saratoga Bridges representative.

It is the policy of Saratoga Bridges that (except for disclosures made for treatment purposes) all disclosures of protected health information (PHI) must be limited to the minimum amount of information needed to accomplish the purpose of the disclosure.

It is also the policy of Saratoga Bridges that all requests for PHI (except requests made for treatment purposes) must be limited to the minimum amount of information needed to accomplish the purpose of the request.

For purposes of this policy, PHI is defined as any information that is created or maintained by Saratoga Bridges that relates to the past, present, or future physical or mental health condition of an individual, the provision of care to an individual, or the past, present, or future payment for the provision of care to the individual. It includes any information that identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual. PHI may include, but is not limited to, the individual's name, address, birth date, social security number, benefit information, medical information, service plans, records of treatment or service delivery, and photographs or other images.

Saratoga Bridges has identified the following safeguards to protect individuals from unauthorized disclosure of PHI.

Verbal Communication
Details concerning individuals, their health information, or information related to service provision should not be discussed in a public area where others may overhear the information. Public areas may include but are not limited to hallways, parking lots, rest rooms, break rooms, and public facilities.

Employees, volunteers, or contractors may not discuss information about individuals served with any unauthorized person, whether on- or off-duty.

Consumer Records/Information
Each employee or contractor is granted access to PHI based on the assigned job functions of the employee or contractor.

All records containing PHI or pertaining to individuals served must be maintained in a secure area, accessible to employees or contractors authorized for such access.

Records stored in general areas will be secured at all times when authorized employees are not in attendance.

Information stored in offices or program areas must be secured and accessible to authorized personnel only.

Employees must maintain a clean desk practice; no PHI may be left unattended on desks or other areas in a manner that is visible to others. Desks and surfaces must be cleared of PHI at the end of the shift/day. Records should be secured in locked drawers or cabinets.

Information pertaining to individuals may not be visibly posted on walls, bulletin boards, etc. This includes but is not limited to rosters, schedules, service needs, and health or medication needs.

Confidential information to be reviewed at meetings shall not be routinely distributed prior to meetings. If it is necessary to distribute confidential information prior to meetings, the following precautions should be observed:

- The material should be clearly marked as confidential;
- Distributed copies of the confidential information should be numbered;
- Each copy should be retrieved at the meeting at which it is reviewed;
- All numbered copies should be destroyed; and
- The original should be retained in a secure location.

Employees or committee members who maintain records of the meetings must assure that the records are safeguarded at all times and that any records are returned to the Organization for destruction or upon separation from the committee or function.

Removal of Records From Saratoga Bridges Premises
Records or information pertaining to individuals may not be removed from the facility without the prior approval of a supervisor with authority over the records.

Employees or contractors will be responsible to sign out any records removed from the facility and complete the documention upon return of the records.

Employees or contractors are responsible for the safeguarding of records in their possession. No records may be left unattended or unsecured in a manner that will allow access by unauthorized parties.

Employees and contractors must report the loss or destruction of any records to the supervisor with authority over the records immediately upon loss or destruction.

Computer Use and Access
Computer use and access is determined by job functions. Only authorized persons may access Saratoga Bridges computers or network.

Employees or contractors may not share passwords or identity with any other person or allow another person access to the computer with their password.

Human Resources personnel must be notified immediately upon the decision to terminate an employee or contractor in order to initiate access restrictions.

Information pertaining to individuals served may not be loaded onto other computer systems without the approval of the Information Security Officer and the appropriate safeguards to prevent unauthorized access or disclosure.

Computer screens should be shielded or located in a manner that prevents access by unauthorized personnel.

Employees or contractors must exit any programs or files containing PHI before leaving the computer unattended. Password protected screensaver should be utilized when computers are unattended.

All e-mail messages must contain a confidentiality statement and include the identity of the Saratoga Bridges employee or contractor sending the message.

No PHI should be emailed outside of Saratoga Bridges network unless it is encrypted.

Missing or stolen laptops or other portable devices must be immediately reported to Information Security Officer or Privacy Officer.

Fax Protocol
All fax transmissions must include a cover memo including the name and phone number of both the sender and the recipient. All cover memos must include a confidentiality statement.

Fax machines should be located in a supervised area to prevent unauthorized access or disclosure of confidential information.

Authorized personnel should remove faxes and deliver to the recipient directly or place the document in an interdepartmental envelope for delivery.

Fax machines should be monitored on a routine basis for the receipt of messages.

Printer Protocol
Employees or contractors are responsible for retrieving print jobs containing confidential information promptly upon printing.

Authorized personnel who remove print jobs from a shared printer should deliver the material to the recipient directly or place the information in an interdepartmental envelope for delivery.

Mail Protocol
Personnel are designated by job function to distribute mail within Saratoga Bridges.

All interagency mail must be placed in an interdepartmental envelope and include the name of the recipient.

Employees and contractors are responsible to remove mail from mailboxes on a regular basis. During absences, other personnel should be assigned the responsibility for retrieving and securing the mail.

Employees or contractors should not open the mail of others unless authorized to do so by the appropriate program administrator.

Cellular Phones and Mobile Devices
Mobile devices should not be used to email PHI unless the device has been encrypted and Saratoga Bridges has authorized such use. Email by its very nature uses an unsecure protocol. There are a number of risks, including the possibility of data interception.

Missing or stolen mobile devices must be reported immediately to the Information Security Officer or the Privacy Officer.

Social Media
Employees and contractors are prohibited from posting or including PHI or any information about individuals on social media (i.e., Facebook, YouTube, Twitter).