Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Acceptable Use*

Policy Purpose:

The purpose of this policy is to outline the acceptable use of computer equipment at **Saratoga Bridges**. These rules are in place to protect the employee and **Saratoga Bridges**. Inappropriate use exposes **Saratoga Bridges** to risks including virus attacks, compromise of network systems and services, and legal issues.

This policy applies to employees, contractors, consultants, temporaries, and other workers at **Saratoga Bridges**. These rules are in place to protect the employee and **Saratoga Bridges**. Inappropriate use exposes **Saratoga Bridges** to risks including virus attacks, compromise of network systems and services, and legal issues.

Policy Description / Responsibilities:

General Use and Ownership

1. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
2. Management requires that any information that is considered legally protected, confidential, sensitive or vulnerable be encrypted.
3. For security and network maintenance purposes, authorized individuals within **Saratoga Bridges** may monitor equipment, systems, and network traffic at any time.
4. **Saratoga Bridges** reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every 90 days.
2. All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended (control-alt-delete keys or Windows logo key + L).
3. Use encryption of information in compliance with the Acceptable Encryption Policy.
4. Information contained on portable computers is especially vulnerable. Special care should be exercised. All portable computers shall be encrypted.
5. All hosts used by the employee that are connected to **Saratoga Bridges** Internet/Intranet/Extranet, whether owned by the employee or **Saratoga Bridges**, shall be continually executing approved virus-scanning software with a current virus database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of **Saratoga Bridges** authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing **Saratoga Bridges** owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by **Saratoga Bridges**.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which **Saratoga Bridges** or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a **Saratoga Bridges** computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any **Saratoga Bridges** account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.
12. Circumventing user authentication or security of any host, network, or account.
13. Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of **Saratoga Bridges** employees to parties outside **Saratoga Bridges**.
16. The use of social media networks of any type on **Saratoga Bridges** networks or equipment.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of ‘junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use or forging of email header information.
4. Solicitation of email for any other email address, other than that of the poster’s account with the intent to harass or collect replies.
5. Creating or forwarding “chain letters”, “Ponzi”, or other “pyramid” schemes of any type.
6. Use of unsolicited email originating from within **Saratoga Bridges** networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by **Saratoga Bridges** or connected via **Saratoga Bridges**’ network.
7. Any discussion or posting of EPHI on social media websites such as Facebook.