Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Device and Media Controls*

HIPAA Regulation:

• *Device and media controls*	§164.310(d)(1)	required
• *Disposal*	§164.310(d)(1)	required
• *Media reuse*	§164.310(d)(1)	required
• *Accountability*	§164.310(d)(1)	required
• *Data backup and storage*	§164.310(d)(1)	required

Policy Purpose:

The purpose of this policy is to ensure that electronic protected health information (EPHI) stored or transported on storage devices and removable media is appropriately controlled and managed.

Policy Description:

Device and Media Protection

Saratoga Bridges shall protect all the hardware and electronic media that contain EPHI. This includes, but is not limited to, workstation computers, laptops, personal digital assistants (PDAs) such as Blackberries and smartphones, USB drives, backup tapes, and CDs.

There shall be procedures that govern the receipt and removal of hardware and electronic media that contain EPHI outside of the secured physical perimeter of a **Saratoga Bridges** facility and the movement of these items within the facility. Procedures shall include maintaining a custody record of hardware and electronic media.

Portable Media Security

EPHI that is placed on portable electronic media shall be encrypted, where possible, so that access to the EPHI can only be attained by authorized individuals with knowledge of the decryption code.

Workforce members shall limit the quantity of EPHI on portable electronic media to the minimum necessary for the performance of their duties.

All workforce members shall receive permission from their supervisor before transporting EPHI outside of the secured physical perimeter of a **Saratoga Bridges** facility. Approvals shall include the time period for authorization, which shall be a maximum of one year. **Staff must present removable media for inspection during ISO audits or at any time required for backup.**

Workforce members shall not leave portable media that contains EPHI visible in their vehicles or in any other unsecured location.

If portable media is lost, workforce members are responsible to **immediately** notify their supervisor, the HIPAA Privacy Officer, the Compliance Officer and the Information Security Officer.

Electronic Media Disposal

Before electronic media that contains EPHI can be disposed, the following actions shall be taken on devices by the workforce:

1. Hard drives shall be either wiped clean by IT or destroyed to prevent recognition or reconstruction of the information. The hard drive shall be tested to ensure the information cannot be retrieved.
2. PDAs shall have all stored EPHI erased or shall be physically destroyed.
3. Storage media such as backup tapes, USB flash drives and CDs, shall be physically destroyed (broken into pieces) before disposing of the item.

Electronic Media Reuse

All EPHI shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the EPHI. Hard drives shall be wiped clean by IT before transfer.

All other media shall have all the EPHI removed (the mechanism may vary depending on the media type) and tested to ensure the EPHI cannot be retrieved. If the media is not "technology capable" of being cleaned, the media shall be overwritten or destroyed.

Device Maintenance and Repair

When the technology is capable, all EPHI shall be removed from the device's memory or hard drive before the device is accessed for maintenance externally or sent out for repair. Devices include computer servers, copiers, printers, and other devices capable of storing electronic data.

Device and Media Acquisition

ORGANIZATION shall include security requirements and/or security specifications in information system acquisition contracts based on an assessment of risk (applications, servers, copiers, etc.).

Policy Responsibilities:

Manager and Supervisor Responsibilities

1. Ensure that only workforce members whose duties require the need to transport EPHI outside of the secured physical perimeter of a **Saratoga Bridges** facility are granted permission to do so.
2. Enforce procedures to govern the receipt and removal of hardware and electronic media that contain EPHI outside of the secured physical perimeter of a **Saratoga Bridges** facility and the movement of these items within the facility.

IT Support Responsibilities

1. Ensure that all hard drives are wiped clean of EPHI before disposal, reuse, or being sent out for repair.
2. Maintain an inventory and record of movements of hardware and electronic media such as workstation computers, servers, or backup tapes.

Workforce Member Responsibilities

1. Follow the procedures that govern the receipt and removal of hardware and electronic media that contain EPHI.
2. Limit the quantity of EPHI on portable electronic media to the minimum necessary to perform their duties.
3. Secure EPHI on portable electronic media through encryption.
4. Remove and destroy all EPHI from portable electronic media when it is no longer needed to perform their duties.
5. Do not leave or store portable media that contains EPHI in their vehicles or in any other unsecured location.
6. Report lost/stolen EPHI material immediately.
7. Ensure that portable devices, including cell phones, which contain EPHI are secure. If there is a question, the staff should direct their concerns to the ISO, Compliance Officer or HIPAA Privacy Officer.