	Security	Rio Grande Valley HIE	Policy: S13
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: **Physical Safeguards – Workstation Security**			

FEDERAL REGULATION:

45 CFR 164.310(c)
45 CFR 164.530(c)

POLICY:

Rio Grande Valley Health Information Exchange (RGV HIE) has adopted this policy to establish the physical safeguards applicable for all hardware that may be used to access, transmit, store or receive ePHI, to ensure that appropriate security is maintained and that access is restricted to authorized users. If any of the measures stated in this policy is not supported by the device operating system or system architecture, one of the following steps must be taken:

- The device must be upgraded to support all of the following security measures
- An alternative security measure must be implemented and documented
- The device must not be used to send, receive, or store ePHI

PROCEDURE:

Workstation Security Requirements

- System administrator or root accounts must be changed from the default and password protected using the standards established under RGV HIE Policy S15 Technical Safeguards – Access Control.
- User identification and password authentication mechanisms shall be implemented to control user access to the system, using the standards established in RGV HIE Policy S15 Technical Safeguards – Access Control
- All devices used to access, transmit, receive or store ePHI shall be appropriately secured and protected by boot-level encryption.
- Workstations shall comply with the safeguards established in Protection from Mallicious Software section of this policy
- Workstations shall be configured to receive automatic updates without prompting to ensure all relevant security patches and updates are applied without delay and known vulnerabilities are corrected.
- Workstations shall be located in an area accessible only by employees and comply with physical safeguards outlined in this policy. *See RGV HIE Policy S11 Physical Safeguards – Facility Access Controls*
- Workstations that are located in open, common, or otherwise insecure areas must also implement the following measures:

    - An inactivity timer or automatic logoff mechanism must be implemented. See RGV HIE Policy S15 Technical Safeguards – Access Control
    - The workstation screen or display must be situated in a manner that prohibits unauthorized viewing
    - The use of a screen guard or privacy screen is recommended
- Remote access to RGV HIE workstations is not allowed.

Mobile Devices

- System administrator or root accounts must be changed from the default and password protected using the standards established in RGV HIE Policy S15 Technical Safeguards – Access Control.
- User identification and password authentication mechanisms shall be implemented to control user access to the system, using the standards established in RGV HIE Policy S15 Technical Safeguards – Access Control
- Mobile devices must use a boot password to ensure that the system is only accessible to authorized users. See RGV HIE Policy S15 Technical Safeguards – Access Control
- A virus detection system must be implemented and updates set to automatically download to ensure that the virus detection software is maintained and up-to-date, and comply with as many of the measure established in the Malicious Software section as is allowed by the device and operating system architecture.
- An inactivity timer or automatic logoff mechanisms must be implemented. See RGV HIE Policy S15 Technical Safeguards – Access Control.
- Mobile devices shall not be used for long-term storage of ePHI. ePHI stored on handheld mobile devices must be purged as soon as it is no longer needed on that device, with a storage time not to exceed 30 days.

Removeable storage devices and external equipment are not authorized to store, access, transmit, receive, or send ePHI.

Protection from Malicious Software

The Security Officer will develop mechanisms to guard against and detect new and potential threats from malicious code such as viruses, worms, denial of service attacks or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.

- RGV HIE staff will install virus detection software on all RGV HIE devices and configure for automatic updates.
- The Security Officer shall routinely review to ensure the comprehensiveness of the software protection and that only approved software is being used.
- Employees shall not download any software from the Internet or load any personal or other software programs not approved by RGV HIE.
- The Executive Director or his designee are the only authorized personnel to load software programs on any RGV HIE devices.
- Employees should never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. These attachments should immediately be permanently deleted.
- Employees should delete spam, chain, and other junk email without forwarding.
- Employees shall not use external media devices (e.g. diskette, zip drive, CD ROM) without appropriate approval and inspection as described in RGV HIE Policy S12 Workstation Use.

- Removable storage devices and external equipment should always be scanned for viruses before using.
- The RGV HIE Executive Director or his designee shall ensure that any system that has been infected by a virus, worm or other malicious code is immediately isolated from the rest of the network and properly cleaned.

Disposal/Reuse of Workstations
All hardware shall comply with the Disposal/Reuse of Workstations section of RGV HIE Policy S14 Physical Safeguards – Device and Media Controls.

VIOLATIONS
Any individual found to have violated this policy may be subject to disciplinary action up to and including termination of employment.