RGVHIE Rio Grande Valley Health Information Exchange	**Security**	**Rio Grande Valley HIE**	**Policy: S12**
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: **Physical Safeguards – Workstation Use**			

<u>FEDERAL REGULATION</u>:

45 CFR 164.310(b)

<u>POLICY</u>:

Rio Grande Valley Health Information Exchange (RGV HIE) is committed to conducting business in compliance with all applicable laws and regulations. RGV HIE has adopted this policy to outline the physical measures required to protect electronic information systems and related equipment from unauthorized use. This policy is to specify proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

<u>PROCEDURE</u>:

Compliance

RGV HIE employees agree to support and abide by established standards and conditions of data integrity and data exchange when they sign the workstation use policy and accept RGV HIE devices (see HHR_007 Electronic Media).

RGV HIE devices and media are used to support onboarding, monitoring, education, training, administrative and other RGV HIE functions as defined by the board.

- Remote access to RGV HIE devices and media is not allowed.
- For disposal and reuse, see RGV HIE Policy S14 - Device and Media Controls.

<u>Definitions of device and media types</u>

- **Workstations**: RGV HIE issued laptops.
    - RGV HIE workstations are authorized to send, receive, store or access ePHI and must be in compliance with RGV HIE Policy S13 – Workstation Security.
    - RGV HIE employees shall take reasonable and appropriate steps to secure any workstation used by an employee at all times to prevent unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information.
    - Visitors are denied access to RGV HIE workstations.
- **Mobile Devices**: RGV HIE issued tablets, phones and other handheld devices.

  - RGV HIE mobile devices are authorized to send, receive, temporarily store or access ePHI and must be in compliance with RGV HIE Policy S13 – Workstation Security.
  - RGV HIE mobile devices shall not be used for long-term storage of ePHI.
  - ePHI stored on RGV HIE 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.
  - Visitors are denied access to RGV HIE mobile devices.
- **Removable Storage Device**: Includes but not limited to, disk drives, tapes, disks, flash cards, USB memory sticks and hard copies.
  - Flash devices are solid state and are non-volatile so the memory maintains data even after all power sources have been disconnected. Examples include thumb drives, CompactFlash, Memory Stick, Secure Digital, SmartMedia and other types of plug-ins, and a range of mini and micro-drive flash devices that use USB or FireWire ports.
  - Neither degaussing nor over-writes offers absolute guarantee of non-recoverable erasure. For this reason, these devices are high risk breach devices and are NOT authorized to store or access ePHI.
- **External Equipment**: Workstations, mobile devices or removable storage devices that are personal or were not issued by RGV HIE.
  - External equipment are high risk breach devices, storing, accessing, transmitting, receiving or sending ePHI is strictly forbidden on these devices.
  - Employees who require use of external equipment to support their job responsibilities must have authorization from the CEO to bring the equipment into the workplace.
  - External equipment connected to the RGV HIE network must be inspected and approved for use by the ISO and are subject to re-inspection at any time as long as the external equipment is needed to support job responsibilities.
  - Employees bringing external equipment to the RGV HIE workplace and/or is connected to the RGV HIE network, are responsible to adhere to the guidelines set forth in the HHR_007 Electronic Media policy.
  - Employees agree to maintain such equipment/media devices in accordance with RGV HIE Policy S13 – Workstation Security, which includes the installation and updating of current antivirus software.
  - Failure to comply with any of the aforementioned guidelines will result in prohibition of said external equipment in all RGV HIE offices.
  - An employee may be held financially and criminally liable for failure to maintain external equipment and/or usage of non-approved external equipment which results in the destruction, interruption, and/or breach of integrity of ePHI or the RGV HIE network.
  - Connecting visitor external equipment to RGV HIE workstations, mobile devices or removable storage is denied.

Implementation

- All RGV HIE codes of conduct apply to information technology as well as to other forms of communication and activity.
- The ISO is empowered to suspend some or all privileges associated with computer use in cases of misuse or threat to the integrity of all or part of the RGV HIE information management resource.
- Before any permanent action is taken against a user, the user will be advised of the basis for the proposed action and given an opportunity to respond.

- Where a violation of RGV HIE policies or applicable law appears to warrant action, the matter shall be referred to the appropriate administrative party and or law enforcement.
- Complaints or concerns about another's use of RGV HIE's computer resources should be directed to the CEO or ISO.
- Workstations, servers and mobile devices shall be restricted by user identification and password authentication mechanisms. (see RGV HIE Policy S13 Workstation Security and RGV HIE Policy S15 Access Control)
- Each employee is responsible for any and all access to the network resulting from the use of their individual access control and password.
- It is recommended that food, and especially drinks, should not be kept in close proximity to the computer, keyboard, mouse or CPU.

Monitoring

RGV HIE employees or visitors that use RGV HIE assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, RGV HIE may log, review, or monitor any data (ePHI and non-ePHI) accessed, stored or transmitted on its information system assets.

VIOLATIONS:

RGV HIE may remove or deactivate user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

See RGV HIE Policy S8 Security Incident Procedures for breaches or violations of this policy.

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