	Security	Rio Grande Valley HIE	Policy: S11
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: **Facility Access Controls**			

FEDERAL AND STATE LAWS AND REGULATION:

45 CFR 164.310(a)(1) and (2)

POLICY:

Rio Grande Valley HIE (RGV HIE) has adopted this policy to ensure that physical access to ePHI is appropriately controlled. This policy covers the procedures that will limit physical access to its facilities containing information systems having ePHI or software programs that can access ePHI while ensuring that proper authorized access is allowed. This policy is consistent with the RGV HIE Risk Assessment.

Business Hours

- Regular Business Hours: RGV HIE shall identify its regular hours of office operation which are Monday through Friday (excluding holidays) 9AM to 5PM.
- After Hours: Any time other than Regular Business Hours, including Monday through Friday before 9AM and after 5PM, all day on holidays and weekends.

Facility Spaces

- Check-in area: RGV HIE front lobby and front desk area up to the portal to the hallway.
- Office area: All rooms beyond the check-in area including offices, help desk area and conference rooms.

PROCEDURE:

Facility Access Controls (164.310(a)(1))

The RGV Facility Security Plan, as documented in the Risk Assessment, outlines procedures to limit physical access to its electronic information systems and the facility in which they are housed, while ensuring that properly authorized access is allowed. RGV HIE has documented potential risks and vulnerabilities in the Risk Assessment, as well as risk management procedures. The level of protection for RGV HIE information systems containing ePHI is commensurate with that of identified risks.

- Facility Physical Controls
  - RGV HIE employees may access the office at any time.
  - Visitors and vendors whether solicited or unsolicited may enter the check-in area during regular business hours.

    - RGV HIE office entrance shall be locked after hours and during regular business hours when the facility is vacant.
    - RGV HIE employees that require access to the office after business hours must keep the entrance locked at all times.

- Facility Vulnerabilities
    - Locked back door opening into shared area with restroom
    - Printers and fax machines are located in open areas.
    - Laptops and mobile devices have more risk than desktop computers due to their portability.
    - Workstations in open area are susceptible to public access and viewing.
    - Visitors, vendors, contractors and other non-employees entering RGV HIE can be a vulnerability.

Contingency Operations 164.310(a)(2)(i)
Procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of emergency include:

- Executive Director shall coordinate facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.
- The Executive Director is responsible for access to ePHI during a disaster.
- RGV HIE shall comply with the guidelines established in RGV HIE Policy S9. Administrative Safeguards - Contingency Plan.

Facility Physical Controls 164.310(a)(2)(ii)
Procedures to safeguard the facility and the equipment from unauthorized physical access, tampering, and theft include:

- Front and back doors locked
- Deadbolt on the back door, which opens onto common area and restrooms
- Locked file cabinets
- Cleaning service conducted under supervision of RGV HIE staff.
- Paper documents containing PHI are shredded and disposed of using shredding service
- Limited PHI stored, received, maintained or transmitted by staff in RGV HIE office, as identified in the RGV HIE Risk Assessment.
- Maintain an inventory list that identifies systems containing ePHI, and shall document in the Risk Assessment.
- RGV HIE staff each have a laptop which is inventoried in our IT equipment log. RGV HIE does not have desktop computers.

- All workstations, laptops and other RGV HIE issued devices shall comply with RGV HIE Policy S13 - Workstation Use and RGV HIE Policy S13 - Workstation Security to guard against theft or loss.

- ePHI will not be accessed on any device not issued by RGV HIE under any circumstances or on any device that is not able to or does not comply with RGV HIE Policy S13 - Workstation Security.

Access Controls and Validation 164.310(a)(2)(iii)
Procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision include:

- RGV HIE cleaning service does not have keys or other access to enter the facility without supervision.

- Visitors and vendors needing access to RGV HIE office areas may enter the office area only after verification, sign-in at the front desk and if accompanied by a RGV HIE employee at all times.

- Employees shall be extra vigilant when non-employees are in the office areas and around the printers, fax machines and mobile devices.

- RGV HIE staff, employees and workforce members needing access to RGV HIE systems containing ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms, shall comply with RGV HIE Policy S5 - Workforce Security.

- Extra consideration for requests for outside user, vendor and visitor access shall comply with RGV HIE Policy S6 – Information Access Management.

- RGV HIE shall comply with guidelines established in RGV HIE Policy S15 - Access Control.

- RGV HIE shall monitor physical access to the information systems containing ePHI to detect and respond to physical security incidents as outlined in RGV HIE Policy S8 - Security Incident Procedures.

- RGV HIE Privacy and Security Officers shall periodically review audit logs generated from system monitoring.

Maintenance Records 164.310(a)(2)(iv)
Procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks) include:

- Vendors and contractors making repairs or modifications to the physical components of the RGV HIE facility, may enter the office area only after verification, sign-in at the front desk and if accompanied by a RGV HIE employee at all times.

- All repairs, modifications and maintenance that are related to the security of PHI shall be documented at the front office. Repair or modification documentation shall be maintained in a secure manner and shall include:

    - Date and time of repair or modification
    - Reason for repair or modification
    - Name and company of technician performing the repair
    - Outcomes of the repair

- The Executive Director shall explicitly approve the removal of system components from the RGV HIE facility for off-site maintenance or repairs.
- RGV HIE shall comply with the guidelines established in RGV HIE Policy S14 - Device and Media Controls and sanitize equipment to remove all information from associated media prior to removal from the office for off-site maintenance.

VIOLATIONS:

Any individual, found to have violated this policy or any security measure, is subject to disciplinary action up to and including termination of employment. Any incident shall be reported in compliance with S8 Security Incident Procedures.