	Security	Rio Grande Valley HIE	Policy: S5
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: **Administrative Safeguard - Workforce Security**			

FEDERAL REGULATION:

45 CFR 164.308(a)(3)

POLICY:

Rio Grande Valley Health Information Exchange (RGV HIE) has adopted this policy to establish mechanisms to ensure that only trained individuals (including employees) who are authorized to access its ePHI have appropriate authorization, clearance and supervision and shall include the following components:

- **Authorization and/or Supervision 164.308(a)(3)(A)** – RGV HIE shall identify workforce members having legitimate need for specific information in order to accomplish their assigned job responsibilities.
- **Workforce clearance 164.308(a)(3)(B)** – RGV HIE shall determine that workforce member access to ePHI is appropriate, and meets the standards set in this policy.
- **Termination 164.308(a)(3)(C)** – RGV HIE shall identify mechanisms to determine under what circumstance current and former employees (or other users) may have access to ePHI

PROCEDURE:

RGV HIE ensures that access to systems containing ePHI is assigned and managed in a manner commensurate with the role of each employee and consistent with the HIPAA Privacy and Security rules.

Authorization and/or Supervision

Workforce members who need direct access to RGV HIE systems containing ePHI to accomplish legitimate job responsibilities shall obtain access authorizations in accordance with RGV HIE Security Policy S6 Administrative Safeguards - Information Access Management. Workforce members who work in locations where ePHI might be accessed and who do not need direct access to ePHI to accomplish legitimate job duties or responsibilities shall be supervised by an individual physically present with authority for the area being accessed.

- As a result of employment with RGV HIE, employees needing legitimate access in order to accomplish their assigned job responsibilities shall have access to the applications requested in the System Access Request form.

- No employee is permitted to authorize their own access or be granted authorization by anyone other than the Privacy Officer. The Privacy Officer must approve any changes to access by an employee.

Workforce Clearance Procedure

- **Background Checks**: All new staff, volunteer and intern positions are required to have an employment background check.

- **Employment Decisions**: In making a final decision about employment, the following shall be considered, at a minimum:

    - Results of an employment background check.
    - Confirmation of prior employment and educational references.

- **Position Description**: When defining a position, the Executive Director shall identify the security responsibilities and supervision required for the position. Security responsibilities include general responsibilities for implementing or maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of RGV HIE systems or processes.

- **Business Associate Agreement**. The Executive Director is responsible for verifying that a third party contracted for services has executed a Business Associate Agreement (BAA) before ePHI is accessed.

- **Confidentiality Statement**: Workforce members who are authorized to access RGV HIE systems containing ePHI must sign a confidentiality agreement. The confidentiality agreement shall affirmatively set forth individual responsibility for protecting confidentiality, integrity or availability of RGV HIE systems and processes and possible sanctions for violations.

- **Training*:*** Prior to receiving access to the system, workforce members must attend appropriate training related to privacy and security policies and procedures, including password maintenance, incident reporting, virus protection etc.

Termination Procedure

Upon notification of employee termination or intent to terminate, the Executive Director is responsible for notifying appropriate staff of the termination / intended termination. The Executive Director or his designee shall disable access to programs no later than the employee's final day of work. The Executive Director or his designee is responsible for ensuring:

- Access to all RGV HIE systems that contain ePHI as well as others shall be disabled.

- The terminating employee returns all keys, badges, access cards, or other facility access control mechanisms.

- All RGV HIE laptops, PDAs, discs, memory cards, flash drives, etc. are turned in prior to, or on the last day of employment.

- All non-business related information such as emails, schedules, etc, found on the computers, laptops, PDA, etc., shall be deleted prior to the equipment being used by another employee.

- Codes for key punch systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate

Access to ePHI or any RGV HIE network domain shall not be extended to any employee beyond the termination date unless a Business Associates Agreement is established with the terminating employee.

VIOLATIONS

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