	Security	**Rio Grande Valley HIE**	**Policy: S8**
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: **Administrative Safeguard – Security Incident Procedures**			

FEDERAL REGULATION:

45 CFR 164.308(a)(6)

POLICY:

Rio Grande Valley Health Information Exchange (RGV HIE) workforce members and RGV HIE data users, shall promptly report any suspected or observed security incident or violation that may impact the confidentiality, integrity or availability of its ePHI. A security incident is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or the interference with system operations in an information system. 164.308(a)(6)(i)

This Policy covers the Incident Response and Reporting System to address the harmful effects of security incidents that are known to RGV HIE, in accordance with federal regulations which includes:

1. Response and reporting of HIPAA security incidents.
2. Documentation of Security Incidents.
3. Mitigation of harmful effects of known security incidents.

164.308(a)(6)(ii)

PROCEDURE:

1. Response and reporting of HIPAA security incidents

- RGV HIE requires prompt reporting of any suspected or observed incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI using the following procedures:
  - RGV HIE shall notify employees, trainees, and volunteers of new and potential threats from malicious code such as viruses, worms, denial of service attacks, and any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.

  - RGV HIE shall investigate and propagate recommended updates or fixes to threatened or actual security incidents.

- All individuals given access to the handling of ePHI under RGV HIE must notify RGV HIE Executive Director of issues involving viruses, local attacks, denial of service (DOS) attacks, etc. Incidents that should be reported include, but are not limited to:
    - Virus, worm, or other malicious code attacks
    - Network or system intrusions
    - Persistent intrusion attempts from a particular entity
    - Unauthorized access to ePHI, an ePHI based system, or an ePHI based network.
    - ePHI data loss due to disaster, failure, error

- RGV HIE Executive Director shall aggregate and assess the severity of security incidents involving ePHI and report those incidents, when appropriate.

- The RGV HIE Security and Privacy Officers must notify clients of security or privacy issues if they determine that an incident or issue could involve them.

- RGV HIE shall adhere to the protection from malicious software procedures established in HIPAA Policy S12 - Workstation Use.

- RGV HIE shall adhere to the Risk Determination procedures as established in HIPAA Policy S01-Risk Analysis and Management. RGV HIE shall adhere to the password procedures as established in HIPAA Policy S15 – Access Controls.

2. **Documentation of Security Incidents**. RGV HIE shall document all security incidents including the date, time, description of incident, responsible parties, ePHI impacted, any mitigation efforts, and whether incident was reported.

3. **Mitigation of Harmful Effects of Known Security Incidents**. RGV HIE will identify any harmful effects and take appropriate steps in compliance with all requirements to mitigate any harmful effects.

<u>VIOLATIONS</u>

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