	Security	Rio Grande Valley HIE	Policy: S17
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: **Technical Safeguards – Integrity**			

FEDERAL REGULATION

45 CFR 164.312(c)

POLICY

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 mechanisms to appropriately protect electronic protected health information from improper alteration or destruction in any unauthorized manner. RGV HIE and its technology vendors are committed to using industry accepted security standards for developing our security posture. Security compliance is an ongoing process for increasing and ensuring compliance with standards.

PROCEDURE:

RGV HIE will require technology vendors to implement appropriate data authentication measures in compliance with HIPAA to ensure that ePHI is not improperly altered or destroyed. RGV HIE and its technology vendors will use data authentication to validate data integrity, verify that the data sent is the same data that is received, and ensure the integrity of data stored and retrieved.

Authentication Integrity
The Security Officer will implement mechanisms, and will require technology vendors to implement mechanisms, to track organization users and roles, audit access, and train users who are authorized to access ePHI. *See RGV HIE Policy S5. Administrative Safeguards - Workforce Security, RGV HIE Policy S7. Administrative Safeguards - Security Awareness and Training, RGV HIE Policy S15. Technical Safeguards - Access Control*.

Transmission Integrity
The Security Officer will implement mechanisms, and will require technology vendors to implement mechanisms, to corroborate that ePHI is not altered or destroyed during transmission. *See RGV HIE Policy S15. Technical Safeguards - Access Control*

System Integrity
The Security Officer shall implement, and require technology vendors to implement, mechanisms to ensure that ePHI is not altered or destroyed by a virus or other malicious code. *See RGV HIE Policy S7 Administrative Safeguards - Security Awareness and Training, RGV HIE Policy S13. Physical Safeguards - Work Station Security, and RGV HIE Policy S15. Technical Safeguards - Access Control*

Data at Rest Integrity
The Security Officer will implement mechanisms, and require technology vendors to implement mechanisms, such as error-correcting memory and storage to authenticate data that is being stored and retrieved. For

medium and high-risk ePHI, a DES (digital encryption standard), encryption mechanism, or data check may be used to ensure the integrity of the data at rest. The use of data authentication mechanisms other than virus detection is not required for low risk ePHI. *See RGV HIE Policy S13. Physical Safeguards - Work Station Security.*

VIOLATIONS

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