	Security	Rio Grande Valley HIE	Policy: S16
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: **Technical Safeguards – Audit Controls**			

FEDERAL REGULATION:

45 CFR 164.312(b)

POLICY

Rio Grande Valley Health Information Exchange (RGV HIE) has adopted this policy to set forth the hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. This policy covers hardware, software and/or procedural mechanisms that will be implemented by RGV HIE to record and examine activity in information systems that contain or use ePHI.

PROCEDURE:

All Information Security policies and procedures are subject to periodic audits by the external audit firms, internal audit activities and/or the Information Security Officer. The Information Security Officer shall implement automatic reviews of designated audit review items, and unannounced periodic reviews of areas of concern identified through the regular periodic review process.

Audit Control Mechanisms

The Information Security Officer shall ensure there is a mechanism to log and store activity for each user of the systems containing medium and high-risk ePHI.

- Individual system audit logs shall include, but is not limited to the User ID, Log-in Date / Time and Activity Time.
- Audit logs may include system and application login reports, activity reports, exception reports or other mechanism to document and manage system and application activity.
- System audit logs shall be reviewed on a regular basis by the ISO in accordance with the attached Audit Listing.
- Implementation of an audit control mechanism for systems containing low risk ePHI is not required.

Audit Control and Review

Audit control and review procedures shall be developed by the Information Security Officer and the Privacy Officer in conjunction with the managers of the various services utilizing medium and high-risk ePHI. The procedures should include:

- Systems and applications to be logged
- Information to be logged for each system
- Log-in reports for each system
- Procedures to review all logs and activity reports

Policies

Changes in the inventory, systems or operational procedures shall prompt a review of the procedures by the Information Security Officer.

- Review of Policies & Procedures - Bi-Annually
- Responses to Security Incident – Annually
- Review of Access Levels - Annually

Reports

The Information Security Officer shall report on an annual basis to the Board of Directors, the results of the various audits performed.

Per risk level schedule (see Organization and Audit Inventory.x1sx)

- Log on / Log off
- Passwords
- PHI access
- Active users

Technical

Systems and system reports are reviewed monthly. Included but not limited to:

- User Access (see IT-UAADMIN002-Access Tracker.x1sx)
- Back-ups
- ePHI systems
- Malware/spyware
- Anti Virus
- Help Desk Testing