


|   |                                     |  |   |
|---|-------------------------------------|--|---|
|  | <b>Security</b>                     | <b>Rio Grande Valley HIE</b>                   | <b>Policy: S1</b>                         |
|   | <b>Effective Date</b><br>11/20/2015 | <b>Last Date Revised/Updated</b><br>11/20/2015 | <b>Date Board Approved:</b><br>11/20/2015 |
| <b>Subject: Administrative Safeguards – Risk Analysis and Management</b>          |                                     |  |   |

**FEDERAL REGULATION AND GUIDANCE:**

45 CFR 164.308(a)(1)(ii)(A), (B), (D)

Guidance on Risk Analysis Procedure under the HIPAA Security Rule (issued by OCR on July 14, 2010)

ONC-HIE-PIN-003. Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program.

**POLICY:**

RGV HIE shall establish a system to prevent, detect, contain and correct security violations relative to its ePHI. This system will address processes to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information. This shall include the development of processes to determine various risks associated with the information system and the management of those risks. This shall include:

- Risk Analysis – the identification, definition and prioritization of risks related to the confidentiality, integrity and availability of its ePHI
- Risk Management – the actions necessary to reduce the risks to ePHI to a reasonable and appropriate level
- Information System Activity Review – procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

**PROCEDURE:**

**Risk Analysis**

RGV HIE will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by RGV HIE. The formal Risk Analysis of the RGV HIE’s and technology vendors’ Information Systems shall include the following elements:

1. Scope of the Analysis and Data Collection. The Risk Analysis will account for all of RGV HIE’s e-PHI, regardless of the particular electronic medium in which it is created, received,

maintained or transmitted or the source or location of its e-PHI. The Analysis will identify and document where the e-PHI is stored, received, maintained or transmitted, including:

- Identification of electronic equipment having the potential for creating, storing or transmitting ePHI
- Identification of where all ePHI is located or where it may be accessed, including where it is stored, received, maintained, or transmitted.
- Identification of all users having access to the Information System
- Identification of all points of access within the Information System
- Identification of the importance or the critical nature of information as it relates to the essential operations of RGV HIE
- Identification of current security systems / measures to protect the Information Systems and ePHI

2. Threat Identification and Documentation. The Risk Analysis should identify and document the potential threats to the Information System based on experience, and potential for activities / events that may have a negative impact on the Information Systems. All reasonably anticipated threats to ePHI will be identified.

3. Vulnerability Identification and Documentation. The Risk Analysis should identify and document vulnerabilities that, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI. The development of a security checklist shall be used to identify potential vulnerabilities.

- Identification of vulnerabilities in the existing system that may result in an accidental or intentional breach of the Information Systems which would create a risk of inappropriate access to or disclosure of ePHI.
- Determination of the likelihood of threats given the existing vulnerabilities and security measures
- Identification of the impact of a given security breach

4. Assessment of Current Security Measures. The Risk Analysis should assess and document the security measures RGV HIE uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. This includes assessing the security measures of technology vendors as part of start-up and implementation activities.

5. Risk Determination. The Risk Analysis will include the following components of risk determination:

- *Determine the Likelihood of Threat Occurrence* - Document all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of e-PHI of RGV HIE participating providers.
- *Determine the Potential Impact of Threat Occurrence* - Document all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of e-PHI within RGV HIE. RGV HIE will determine whether to use a qualitative or quantitative method or a combination of the

two methods to measure the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. The Risk Analysis will use a “risk scale” to determine the overall risk of a potential event.

- *Determine the Level of Risk* - Document the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level. Assign risk levels for all threat and vulnerability combinations identified during the risk analysis.

6. Documentation and Recommendations - Document the risk analysis, and use as a direct input to the risk management process. The risk management recommendations will take into account:

- The degree of risk being addressed
- The operational impact of the recommendation
- The feasibility of the recommendation
- The cost / benefit of the recommendation

Due to the confidentiality of certain information contained within the Risk Analysis, the Analysis shall be retained by the Executive Director and shall not be posted to the website or otherwise be publicly available.

### **Risk Management / Periodic Review and Updates to Risk Assessment**

As a result of the Risk Analysis, RGV HIE shall implement, and contractually require technology vendors to implement, security measures and safeguards sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with HIPAA security rule standards and implementation specifications. The level, complexity and cost of such security measures and safeguards must be commensurate with the risk classification of the various information system repositories and programs.

An integrated risk analysis and management process requires that updates and review of the Risk Analysis occur as part of the planning process for any new technology, not the implementation process, in order to reduce the effort required and ensure the best approach.

In addition to the incorporation of new technology, the Risk Analysis will be reviewed and updated whenever RGV HIE has experienced a security incident, has had change in ownership, and/or turnover in key staff or management. The Risk Analysis will be reviewed at least annually, regardless of whether any events have occurred that would require an update.

### **Information System Activity Review**

RGV HIE will implement, and contractually required technology vendors to implement, Internal audit procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports to ensure that activity for all systems classified as medium to high risk on RGV HIE’s and/or RGV HIE’s vendor Risk Assessments is appropriately monitored and reviewed. RGV HIE’s audit control and review plan is as follows:

- On a regular basis, but no less often than every 90 days, RGV HIE staff will review audit reports of technology vendors documenting information system activity in compliance with HIPAA.

- RGV HIE staff will enter the names of participating providers accessing RGV HIE systems containing PHI into an inventory log and note the level of risk determined for each participating providers.
- RGV HIE staff will evaluate participating providers risk based on turnover rate, participating providers size, staff available to monitor systems, and other factors impacting risk of unauthorized activity.
- The Executive Director will determine the sample size, data elements, and frequency of monitoring information system activity, including audit reports of technology vendors, based on the risk as defined in the participating providers inventory log. The interval of the system activity review must not exceed, but may be less than 90 days.

RGV HIE staff will detect, log, and report immediately to the Security Officer any potential security incidents such as activity exceptions and unauthorized access attempts. If the Security Officer judges the activity as normal operations, RGV HIE staff will document findings in the audit log and set the status to closed. If the Security Officer judges the activity to be an incident, the RGV HIE staff will set the status to incident and escalate to the technology vendor and/or appropriate participating providers leadership. If any Authorized Users are identified as the source of any security violations, the Security Officer will enforce disciplinary actions and comply with incident reporting procedures.

RGV HIE notifies participating providers of RGV HIE's auditing policy in the Services Agreement.