	Security	Rio Grande Valley HIE	Policy: S15
RGVHIE Rio Grande Valley Health Information Exchange	**Effective Date** 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: Technical Safeguards – Access Control			

FEDERAL REGULATION:

45 CFR 164.312(a)

POLICY

Rio Grande Valley Health Information Exchange (RGV) has adopted this policy for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights in compliance with HIPAA Policy S6. Administrative Safeguards - Information Access Management. This policy includes the following:

- **Unique User Identification / Password**. Assign a unique identifier for tracking user identity access to ePHI for the purpose of access control and monitoring use of RGV HIE information system(s).
- **Emergency Access Procedure**. Formal procedures enabling authorized employees to obtain required ePHI during an emergency situation.
- **Automatic Log-off**. Procedures that terminate electronic sessions after a certain period of inactivity on systems that contain or have the ability to access ePHI.
- **Encryption and Description.** Mechanisms to appropriately use encryption to protect the confidentiality, integrity and availability of its ePHI.
- **Wireless Access**. Procedures to prohibit access to RGV HIE networks via unsecured wireless communication mechanisms (e.g. personal computers, cellular phones, PDA, etc.).

PROCEDURE

1. **Unique User Identification / Passwords**
    a. RGV HIE shall assign unique identifiers for user access to systems containing ePHI.
        - RGV HIE shall uniquely identify and track any user granted access to RGV HIE information systems, for the purpose of access control and monitoring access to all networks, systems, and applications, especially those containing ePHI.
        - Any user that requires access to any network, system or application that accesses, transmits, receives or stores ePHI must be provided with a unique user identification (user ID) and password.
        - When requesting access to any network, system or application that accesses, transmits, receives, or stores ePHI, a user must supply their assigned user ID in conjunction with a secure password to gain access.

    b. RGV HIE shall instruct users to follow RGV HIE minimum password security standards when creating passwords.
        - Passwords shall be at least 8 characters in length and should consist of a combination of any three of the following criteria:

    - Any upper case letters (A-Z)
    - Any lower case letters (a-z)
    - Any numbers (0-9)
    - Any special characters (i.e. @,#,$,%,&).
    - Numbers and/or special characters should represent at least two of the 8 characters comprising the password.
- If a system does not support the minimum standards and complexity as defined above, one of the following procedures must be implemented:
    - The password must be adequately complex to ensure that it is not easily guessed and the complexity of the chosen alternative must be defined and documented.
    - The legacy system must be upgraded to support the minimum standards as soon as administratively possible.
    - All ePHI must be removed and relocated to a system that supports the RGV HIE password standards.
- Passwords should be easy to remember but not easy to guess.
- Passwords should not include:
    - Words found in a dictionary.
    - Personal information, names, pets, fantasy characters, etc.
    - Computer terms, commands, sites, company names, hardware, etc.
    - Common usage terms such as slang, jargon, etc.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, l2345abc, etc
    - Any of the above spelled backwards.

c. RGV HIE shall educate users on proper user ID and password use and protection.

- Users shall ensure their user ID and password is appropriately protected and only used for legitimate access to networks, systems, or applications.
- Users are responsible for any and all access to the network resulting from the use of their individual access control and password.
- Users who believe their user ID and/or password has been compromised, must immediately report that as a security incident to the Information Security Officer.
- Users should not use the same password for RGV HIE accounts as for other non-RGV HIE accounts. When possible, the same password for various RGV HIE accounts/programs should not be used. Passwords are to be treated as sensitive and confidential information.
    - Users shall not share their user ID and/or password with anyone, regardless of the circumstance.
    - If someone demands their user ID and/or password or shares their user ID and/or password, refer them to this policy and then contact the Information Security Officer.
    - Users shall not use another person's user ID and/or password to gain access to any software program or network system.
    - Users shall not attempt to learn another person's user ID and/or password.
- Users shall not use the "Remember Password" feature of any application. Users shall not write password down, post or expose to others.
- Users shall not store passwords anywhere in work area.
- Users shall not store passwords in a file or on ANY computer system or mobile device.
- Generic passwords shall not be used on any system containing ePHI.
- Users shall change passwords based on access levels and potential for security breach.
    - Administrator passwords shall be changed on an annual basis or when an administrator leaves the organization.
    - Generic passwords for visitors, volunteers and/or students shall be changed on a semi-annual basis. Inactive accounts using generic passwords shall be disabled until needed.
    - Users may change their password at their discretion – as long as the new

password complies –this policy.

- o Passwords shall be changed if a user believes someone else has gained knowledge of their password.

d. User IDs and/or passwords suspected to have been compromised.

- Must be reported as an incident to the Information Security Officer (see HIPAA Policy S8 – Security incident procedures
- The password must be changed immediately.

e. Employees leaving employment with RGV HIE shall have their passwords deleted no later than their last day of employment. (see HIPAA Policy S03 – Workforce Security)

2. Emergency Access

a. To ensure access to critical ePHI is maintained during an emergency situation, employees should follow the Disaster Recovery and Emergency Mode Operation Policy (HIPAA Policy S9 - Contingency Planning) for retrieval of information and ePHI that would be necessary to provide patient treatment.

b. Electronic information repositories that do not affect patient care are not subject to the foregoing emergency access requirement.

3. Automatic Logoff

a. Servers, workstation, or other computer systems that access or are connected to the RGV HIE network shall employ inactivity timers or automatic logoff mechanisms.

« The aforementioned timers must automatically terminate a user session after a maximum of 15 minutes of inactivity.

- Only in unusual circumstances may a longer period be allowed, which must be approved and implemented by the ISO.

b. Applications and databases using ePHI, must employ inactivity timers or automatic session logoff mechanisms. The aforementioned application sessions must automatically terminate after a maximum of 30 minutes of inactivity.

c. If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures shall be implemented,

- The system must be upgraded to support the required inactivity timer or automatic logoff mechanism
- All ePHI must be removed and relocated to a system that supports the required inactivity timer or automatic logoff mechanism

d. Users must log out or activate the systems automatic logoff mechanism when leaving a server, workstation, application, database system or other electronic system containing ePHI,

3. Encryption & Description

Encryption of ePHI shall be used as an access control mechanism. Encryption of ePHI is required during transmission to ensure integrity of the information. All RGV HIE devices shall be encrypted as outlined in HIPAA Policy S12 – Workstation Security. . There may be circumstances in which encryption is not used as the receiving party may not be able to decrypt the information, such as the following:

- ePHI sent to patients who have requested they receive information via email
- ePHI may not be sent via regular email to entities outside of RGV HIE.

In these instances, only the minimum necessary information should be disclosed / transmitted.

The use of encryption is limited to those algorithms that have received substantial public review and have been proved to work effectively. All Federal regulations shall be followed, and legal authority is granted for the dissemination and use of encryption technologies. RGV HIE's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Information Security Officer. Be aware that the export of encryption technologies is restricted by the U.S. Government.

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

4. Remote Access

RGV HIE employees and authorized third parties can use remote connections to gain access to RGV HIE workstations, for troubleshooting and repair, only with appropriate approval. The employee and third party must take every reasonable measure to protect RGV HIE's resources and confidentiality of information.

Vendor access by third parties shall be monitored and strictly controlled using a one-time password authentication. Third parties must contact the Information Security Officer for approval and to receive the password. The access shall be available only for the specific job.

It is the responsibility of employees with a remote access privileges to ensure a remote connection to RGV HIE is not used by non-employees to gain access to company information system resources. Dial-in access to RGV HIE's network is not authorized.

Requirements

- RGV HIE employees are prohibited from providing their login or email password to anyone, not even faintly members or their supervisor
- Routers for dedicated ISDN lines configured for access to the RGV HIE network must be configured for authentication.
- Split-tunneling or dual homing is not permitted at any time.
- Personal equipment that is used to connect to RGV HIE cloud networks and service must meet the requirements of RGV HIE owned equipment for remote access. Please refer to HIPAA Policy S 11 – Workstation Use.
- The Information Security Officer shall ensure that the remote workstation device being used by any employee requesting remote access to a secure network containing ePHI-based systems and applications meets the security measures detailed in HIPAA Policy S12 – Workstation Security.

5. Wireless Access

Access to the RGV HIE network via an unsecured wireless communication mechanism is prohibited. All wireless Access Points / Base Stations connected to the RGV HIE network must be registered and approved by the Information Security Officer. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e. PC cards) used in RGV HIE laptop or desktop computers must be registered with the Information Security Officer.

All wireless LAN access must use RGV HIE-approved vendor products and security configurations.

Wireless access to RGV HIE networks containing ePHI-based systems and applications is permitted as long as the following security measures have been implemented:

- .All wireless devices comply with RGV HIE standards as defined in HIPAA Policy S 12 - Workstation Use and HIPAA Policy S13 - Workstation Security.

- File sharing is disabled between wireless clients.
- Media Access Control based/security enabled, and SSID/Password authentication must be enabled.
- WEP keys are not allowed.
- All console and other management interfaces have been appropriately secured or disabled
- Unmanaged, ad-hoc, or rogue wireless access points are not permitted on any network segment of RGV HIE
- All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption

The Information Security Officer shall ensure that any request for access to a secure wireless network shall meet the security measures detailed in this policy.