	Security	Rio Grande Valley HIE	Policy: S19
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: Technical Safeguards – Transmission Security			

FEDERAL REGULATION

45 CFR 164.312(e)

POLICY

Rio Grande Valley Health Information Exchange (RGV) has adopted this policy to outline the requirements for transmission of ePHI to ensure the security and integrity and defend against improper access of ePHI. This Policy covers the technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

PROCEDURE:

ePHI Transmission

The following procedures must be implemented to appropriately guard against unauthorized access to or modification of ePHI that is being transmitted from the network to an outside network.

- All transmissions of ePHI from the RGV HIE network to an outside network must utilize an encryption mechanism that is protected by (at minimum) FIPS 140-2 standards and uses (at minimum) FIPS 140-2 encryption software between the sending and receiving entities.
- The receiver must be authenticated prior to transmitting ePHI from the RGV HIE network to an outside network. *See RGV HIE Policy S18. Technical Safeguards - Person or Entity Authentication*.
  - All transmissions of ePHI from the RGV HIE network to an outside network should include only the minimum amount of PHI necessary.
  - For transmission of ePHI from the RGV HIE network to an outside network utilizing an email or messaging system see ePH1 Transmission Using Email or Messaging Systems below.

ePHI Transmission Using Email or Messaging Systems

- Transmission of ePHI from RGV HIE to the subject of the ePHI via email or messaging system is permitted if the sender has ensured that the following conditions are met:
  - The subject of the ePHI has formally authorized RGV HIE to utilize an email or messaging system to transmit ePHI.
  - The subject of the ePH1 has been made fully aware of the risks associated with transmitting ePHI via email or messaging systems to them

    - The subject of the ePHI's identity has been authenticated
    - The email or message contains no excessive history or attachments
- Transmission of ePHI outside the RGV HIE network is done via DirectTrust.
    - If the recipient does not have a DirectTrust account, request an encrypted email from the recipient and reply with the minimum necessary ePHI
    - If the recipient does not have encrypted email technology, create a DirectTrust account
    - Transmission of ePHI within the RGV HIE network via email is not allowed

ePHI Transmission Using Wireless LANs and Devices

- Transmission of ePHI over the RGV HIE wireless network is permitted if the following conditions are met:
    - The wireless devices connecting to the wireless network are authorized and use an authentication mechanism. *See RGV HIE Policy S15 Technical Safeguards - Access Control.*
    - The wireless network uses an encryption mechanism for all transmissions.
- If transmitting ePHI over a wireless network that is not utilizing an authentication and encryption mechanism, the ePHI must be encrypted before transmission.
- The authentication and encryption security mechanism is only effective within the RGV HIE network. When transmitting outside of the RGV HIE wireless network, additional and appropriate security measures must be implemented in accordance with this Policy.

ePHI Transmission Using Electronic Removable Media

- Transmitting ePHI via removable media, including but not limited to: CD ROM memory cards, magnetic tape and removable hard drives, the sending party must:
    - Use an encryption mechanism in accordance with this policy to protect against unauthorized access or modification.
    - Authenticate the person or entity requesting ePH1 in accordance with RGV HIE Policy S18. Technical Safeguards – Person or Entity Authentication
    - Send the minimum amount of said EPH I required by the receiving person or entity

Additional Requirements

- All encryption mechanisms must support a minimum of, but not limited to, 128-bit encryption.
- Before transmitting ePHI electronically, regardless of the transmission system being used, RGV HIE workforce members must take reasonable precautions to ensure that the receiving party is in fact who they claim to be and has legitimate need for receiving ePHI.
- If ePHI being transmitted is not to be used for treatment, payment, or health care operations, only the minimum required amount of ePHI should be transmitted.

Violations

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