H.3.A.v

Emory-specific HIPAA Security Regulations

Title: Remote Access Policy

Purpose: This policy defines standards for remotely connecting to Emory network(s). These standards are designed to minimize the potential exposure to damages that may result from unauthorized use of Emory resources.

This policy applies to remote access connections used to do work on behalf of Emory, including reading or sending email, viewing Intranet resources and accessing Information Systems.

Requirements:

1) It is the responsibility of Emory employees, contractors, vendors and agents with remote access privileges to Emory network(s) to ensure that they comply with Emory policies while accessing the Emory network(s) remotely.

2) Employee Remote Access
   a) Employees must be authorized through approved enterprise mechanisms to remotely access ePHI. These requests must be documented and tracked.
   b) Employees must use only approved enterprise VPN solutions to access internal Emory network(s) securely and not other mechanisms such as dialing into modems attached to desktops.
   c) Personal equipment that is used to connect remotely to Emory networks must meet the following requirements:
      i) Equipment must have anti-virus software installed, and the anti-virus pattern files and software must be kept up-to-date.
      ii) Equipment must be kept up-to-date with the most recent security updates and patches.
      iii) Users must ensure that a personal firewall is installed on their system. The firewall must be configured to block unsolicited inbound connections and must be running at all times.
      iv) Users must not store ePHI on personal systems without explicit permission from their appropriate director/dean/chair/vice president or equivalent. Personal systems that are used to store or process ePHI must comply with Emory’s HIPAA policies.
   d) Users must not disclose any of his or her Emory passwords to anyone, not even family members.
3) **Vendor Remote Access**

a) Departments must submit requests for Vendor access via approved enterprise mechanisms.

b) Requests must be documented and tracked.

c) The enterprise security teams will configure connection and document access method.

d) Vendors who require connectivity via methods other than an approved enterprise VPN solution must document their requirements and submit to Emory security teams for approval.

i) Connection requests not approved by Emory must not be used; the security teams will work with vendors to assist them in implementing approved connectivity methods.

e) Vendors are responsible for notifying Emory of any changes to users or requirements.

f) Vendor must sign a Business Associate’s agreement and document their security measures and methodologies.

g) Equipment that is used to connect to Emory network(s) must meet the following requirements:

i) VPN and LAN-LAN connections must be limited only to required systems through an Emory managed firewall or VPN authorized by Emory security teams.

ii) Equipment must have anti-virus software installed, and the anti-virus pattern files and software must be kept up-to-date.

iii) Equipment used to access the Emory network(s) remotely must be kept up-to-date with the most recent security updates and patches.

iv) Vendor must ensure that their network has implemented strong security measures.

v) Vendors may have a direct connection such as T-1 or Frame Relay. Frame relay must meet minimum security requirements approved by Emory information security and network teams.

This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness.

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.

See: HIPAA Security Regulations: Sanction Policy

**Recommended By:** Emory HIPAA Security Working Group

**Effective Date:** April 20, 2005

**Authorized By:** Emory HIPAA Security Steering Committee