H.1.E.ii

HIPAA Security Regulations

Title: Malicious Code and Software Policy

Security Rule: 164.308(a)(5)

Policy Purpose: To ensure that Emory University workforce members are made aware of and able to appropriately respond to threats and vulnerabilities from malicious code or malicious software (e.g., viruses and worms).

Requirements: In order to implement the purpose of this policy, the following procedures must be observed:

1. A virus detection system must be implemented on all workstations including a procedure to ensure that the virus detection software is maintained and up-to-date.

   See HIPAA Security Regulations: Workstation Security Policy

2. In the event that a virus, worm, or other malicious code or software has infected or been identified on a server or workstation managed by a covered component, the University has the right to disconnect the server or workstation from the network until the system has been appropriately cleaned or rebuilt and approved for reconnection to the network.

3. Each business unit (i.e., “covered component”) must disseminate security reminders to its workforce to make them aware of any of new virus, worm, or other type of malicious code that the entity has determined to be a threat to EPHI.

4. Each business unit is responsible for ensuring that its workforce is appropriately trained to detect, protect against, and report malicious software and to minimize the risk caused by malicious code and software.

5. Each business unit must document the security reminders and the training. documentation should include: the type of reminder or training, the content, the date it was provided, and the audience to whom it was communicated.

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
Date of Last Edit: April 21, 2011
Review Date: April 21, 2011