H.3.E.i/ii

HIPAA Security Regulations

Title: Transmission Security Policy

Security Rule: 164.312(e)(1)

Policy Purpose: To minimize the risk of unauthorized access to or modification of ePHI during transmission over a network via any method, including but not limited to e-mail and FTP, Emory will implement appropriate technologies and practices to secure transmitted ePHI.

Definitions:

“Internal transmission” means transmission of ePHI within the Emory Covered Entities.

“External transmission” means transmission of ePHI to any point outside the Emory Covered Entities approved trusted zones or across an untrusted zone or network to a trusted zone.

Requirements: In order to comply with this policy, the following must be observed.

1. Email

   The use of email is inherently insecure therefore the sender must:

   a. Verify email addresses prior to transmission
   b. Verify intended recipient(s) and appropriate use of “to:”, “cc:”, and “bcc:” fields, since email addresses may not be private
   c. Use only Enterprise Exchange to send/receive ePHI via email
   d. Use a valid Emory Enterprise Exchange email account with a valid reply-to Emory Enterprise Exchange email address
   e. Not send or forward email containing ePHI to accounts outside of the Emory approved systems unless it meets the external transmission policy as articulated below
   f. Not include ePHI in the subject line of the email message
   g. Include in the subject line the fact that the email message contains confidential information
   h. Include an approved confidentiality notice in the email or as an attachment
   i. Not transmit specially protected information (HIV/AIDS, substance abuse treatment, and mental health information) via email
   j. Contact the HIPAA Privacy Officer or ORC if questions regarding email communication of ePHI are raised

Internal Transmission:
ePHI may be transmitted internally via email only through the use of Enterprise Exchange.

Process for Approval – Internal email systems must be approved for transmission of ePHI by the WHSC HIPAA Steering Committee. Applications for approval of an internal system should be submitted to the University’s Office of Research Compliance before forwarding to the Committee. The application must include a completed and signed application checklist in order to be considered by the Committee.

**External Transmission:**

Except as provided herein, ePHI must not be externally transmitted via email, regardless of the email system used for transmission, unless prior approval is obtained from the unit HIPAA coordinator and follows the guidelines listed in section 2 below.

**External transmission to patients** – If externally transmitting a patient’s own ePHI via email to the patient, the transmitting covered component must verify that the patient has signed a “Patient Consent to Means of Communication” form. The form is available online from the Emory University Office of Research Compliance at: http://www.orc.emory.edu/share/forms/hipaa/HIPAA_Communication_Consent_Form.rtf

2. **Other technologies – Internal and External Transmission**

Each ePHI system owner is responsible for providing technologies and documenting procedures with which to secure the transmission of ePHI (including transmission via email and FTP) in accordance with all Emory HIPAA policies and other applicable Emory policies.

Acceptable means will vary depending on the risk assessment. The following must be addressed when transmitting ePHI over untrusted zones or networks (including the Internet):

a. Integrity controls – ensure that data have not been tampered with by unauthorized users in transit and at destination
b. Sender and recipient authentication – ensure that sender and the receiver are the parties they claim to be
c. Access controls – ensure that the sender and receiver have appropriate access to the data
d. Encryption – protection of data confidentiality in transit and at destination
e. Event reporting – system or transmission failure and reporting
f. Audit – trace action appropriate to level of risk
g. Reliability/non-repudiation – verification that the message has been sent and received and that the intended sender and receiver were the parties who claimed to send/receive the message

The individual (or data owner) transmitting the ePHI is responsible for verifying that the recipient is authorized to receive the ePHI as outlined in the University’s “HIPAA Policy Regarding Verification Requirements for Disclosure of PHI” available at http://www.orc.emory.edu/share/policies/hipaa/HIPAA_Verification_Disclosure.pdf
The individual (or data owner) transmitting the ePHI is also responsible for ensuring that any required Business Associate Agreements are in effect when transmitting ePHI to or from 3rd parties.

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

See: HIPAA Security Regulations: Evaluation of Compliance Procedures Policy

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

See: HIPAA Security Regulations: Sanction Policy

Recommended By: WHSC 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