H.5.A

HIPAA Security Regulations

**Title:** Documentation Requirements

**Security Rule:** 164.316(a)

**Purpose:**
To ensure that all Emory HIPAA Security Policies and Procedures be documented and maintained either on paper or in electronic form.

**Requirements:**

1) Any change to HIPAA Security Policies or Procedures must be documented and retained for a period of (6) years from the date of its creation or the date when it was last in effect, whichever is greater.

2) Emory must also document and record any action, activity or assessment that is required to comply with the HIPAA Security Rule, such as the following:
   - risk analysis 45 C.F.R. 164.316(a)(2)(i)
   - security official assignment, 45 C.F.R. 164.308(a)(2)
   - security incidents, 45 C.F.R. 164.308(a)(6)(ii)
   - business associate contracts, 45 C.F.R. 164.308(B) and 164.314.

3) Emory must periodically review and update documentation in response to any environmental or operational changes that affect the security of electronic PHI.

4) Emory must make required documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

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:** March 19, 2009
Authorized By: Emory HIPAA Security Steering Committee
Date of Last Edit: August 20, 2015
Review Date: August 20, 2015