**AS - 08 Evaluation**

***Purpose***

To perform a periodic technical and non-technical evaluation, based initially upon the standards that are implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart. 164.308(a)(8)

**Guidance**

* Review and update Unit HIPAA Policy and Practices for Compliance every five (5) years, or more frequently in response to environmental or operational changes that affect the security of ePHI.
* All Unit policies must either reference or be in adherence with the University’s HIPAA Privacy and Security policies. Units may implement their own procedures for adherence. Any Unit policies must be in accordance with University policy.
* Review and update Unit policies and procedures annually if there is no trigger for more frequent review.
* Identify the individual(s) responsible for determining when evaluation is necessary due to environmental or operational changes.
* Document periodic reviews and updates and archive previous versions. Retain for six years.

**Business Associate Contracts and other Arrangements**

Implementation: A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information. 164.308(b)(1)

**Written Contract or other Arrangement**

Implementation: Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a). §164.314(b)(4).

Ensure that agreements with business associates [2] contain language stating that University ePHI receives appropriate safeguards in accordance with Federal HIPAA Security Standards and the UofL HIPAA Business Associates Policy.

* Ensure that UofL-approved Business Associate Agreements (BAAs) are in place at either a System wide or local level for vendors and third-party service providers with access to UofL ePHI or to systems that contain or access ePHI.
* If a System wide BAA does not exist, one must be executed locally through UofL Procurement Services and retained in the Office of Record at SHS for six years.
* HIPAA entity procedures must include notifying Procurement Services when a HIPAA BAA is needed and when renewing an agreement with an existing HIPAA BAA.