**AS—01 Security Management**

***Purpose***

To manage security vulnerabilities and violations in order to protect the confidentiality, integrity and availability of electronic protected health information (ePHI). 164.308(a)(1)(i)

**Guidance**

Covered entities must implement policies and procedures to prevent, detect, contain and correct security violations.

**Risk Analysis**

Implementation: Conduct an accurate and thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity, and availability (CIA) of electronic protected health information (ePHI) held by the covered entity.

* Identify systems and electronic resources that require protection – inventory list.
* Conduct (by unit or in conjunction with the ISO) periodic risk assessments to understand and document risks to the confidentiality, integrity and availability of ePHI systems and resources.
  + Review and update assessments every three years or more frequently as needed in response to legislative, environmental or operational changes.
  + Risk assessments should take into account potential adverse impact on the University’s finances, reputation and operations.
  + Inform the Information Security Office of completion of all risk assessments.
    - Contact the ISO for assessment assistance at [isopol@louisville.edu](mailto:isopol@louisville.edu).
    - Sample assessment: <https://www.hhs.gov/hipaa/index.html>

**Risk Management**

Implementation: Implement recommendations and security measures to reduce risks and vulnerabilities to an appropriate level and in compliance with 164.308(a).

* Identify controls (policies, procedures, safeguards, technologies) and responsible parties for implementation or each recommendation.
* Document and where possible incorporate these standards and practices when evaluating new hardware, software or processes.

**Sanction Policy**

Implementation: Apply sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

* Take disciplinary or other action in accordance with University policies and guidelines on workforce member who, in the course of their employment, frail to comply with University policy and procedures, including information security policy and procedures.
* Ensure that documentation of violations and application of HIPAA-related sanctions is maintained appropriately and retained for six years.
  + Units are responsible for information Human Resources and/or other areas when submitting documentation with this retention requirement.

**Information System Activity Review**

Implementation: Implement procedures to review records of information system activity, such as audit logs, access reports, and security incident tracking reports on a regular basis.

* Regularly review information system activity and login attempts.
* Maintain documentation of periodic log reviews.
* Retain logs relevant to security incidents for six years. Other logs should be retained for up to 90 days or in accordance with university practice.
* Define and document responsibilities and log review procedures and expectations.