URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #1A

Title:	**RISK ANALYSIS**	**Purpose & Background**	**See Memo Entitled "HIPAA at URI: Introduction to HIPAA and an Overview of HIPAA Implementation at URI" available online at the URI HIPAA website**
Originator (Responsible Department/ Unit):	**URI HIPAA Compliance Oversight Committee**	**Effective Date:**	**05/22/2018**
Applies to:	**All URI Departments and Units Designated as HIPAA "Covered Components" and "Business Associate Components"**	**Revised Date(s):**	

Purpose:

This specification reflects URI's commitment to regularly conduct accurate and thorough analysis of the potential risks to the confidentiality, integrity, and availability of its information systems containing EPHI.

Specification:

URI Covered Entities must regularly (in consultation with and under the direction of URI's Information / HIPAA Security Officer) identify, define and prioritize risks to the confidentiality, integrity, and availability of its information systems containing EPHI. The identification, definition and prioritization of risks to information systems containing EPHI must be based on a formal, documented risk analysis process. URI Covered Entities must conduct a risk analysis of its information systems on a regular basis. Such risk analysis must be used in conjunction with URI's risk management process. URI Covered Entities must also conduct a risk analysis when environmental or operational changes occur which significantly impact the confidentiality, integrity or availability of specific information systems containing EPHI.

Procedure:

1. URI Covered Entities must regularly identify, define and prioritize risks to the confidentiality, integrity, and availability of its information systems containing EPHI.

2. The identification, definition and prioritization of risks to information systems containing EPHI must be based on a formal, documented risk analysis process. At a minimum, URI Covered Entities risk analysis process must include the following:

    a. Identification and prioritization of the threats to information systems containing EPHI.
    b. Identification and prioritization of the vulnerabilities of information systems containing EPHI.
    c. Identification and definition of security measures used to protect the confidentiality, integrity, and availability of information systems containing EPHI.
    d. Identification of the likelihood that a given threat will exploit a specific vulnerability on an URI information system containing EPHI.

e. Identification of the potential impacts to the confidentiality, integrity, and availability of information systems containing EPHI if a given threat exploits a specific vulnerability.

3. URI Covered Entities must conduct risk analysis on a regular basis. Such risk analysis must be used in conjunction with URI's risk management process to identify, select and implement security measures to protect the confidentiality, integrity, and availability of information systems containing EPHI.

4. Judgments used in URI Covered Entities risk analysis, such as assumptions, defaults, and uncertainties, should be explicitly stated and documented.

5. In addition to regular risk analysis, URI Covered Entities must conduct a risk analysis when environmental or operational changes occur which significantly impact the confidentiality, integrity or availability of specific information systems containing EPHI. Such changes include but are not limited to:

   a. Significant security incidents to specific information systems containing EPHI.
   b. Significant new threats or risks to specific information systems containing EPHI.
   c. Significant changes to the organizational or technical infrastructure of URI which affect specific information systems containing EPHI.
   d. Significant changes to URI information security requirements or responsibilities which affect specific information systems containing EPHI.

6. URI's risk analysis process must be based on the following steps, which shall be formally documented and maintained:

   a. **Inventory** - URI Covered Entities must conduct a regular inventory of its information systems containing EPHI and the security measures protecting those systems.

   b. **Threat Identification** - URI Covered Entities must identify all potential threats to its information systems containing EPHI. Such threats may be natural, human or environmental.

   c. **Vulnerability identification** - URI Covered Entities must identify all vulnerabilities on its information systems containing EPHI. This should be done by regularly reviewing vulnerability sources and performing security assessments.

   d. **Security control analysis** - URI Covered Entities must analyze the security measures that have been implemented or will be implemented to protect its information systems containing EPHI; this includes both preventive and detective controls.

   e. **Risk likelihood determination -** URI Covered Entities must assign a rating to each specific risk which indicates the probability that a vulnerability will be exploited by a particular threat. Three factors should be considered:
      1) threat motivation and capability,
      2) type of vulnerability
      3) existence and effectiveness of current security controls

   f. **Impact analysis** - URI Covered Entities must determine the impact to confidentiality, integrity or availability of EPHI which would result if a threat were to successfully exploit a vulnerability on an URI information system containing EPHI.

   g. **Risk Determination** - URI Covered Entities must use the information obtained in the above six steps to identify the level of risk to specific information systems containing EPHI. For each vulnerability and associated possible threat, URI Covered Entities must make a risk determination based on:

      - The likelihood a certain threat will attempt to exploit a specific vulnerability.
      - The level of impact should the threat successfully exploit the vulnerability.

- The adequacy of planned or existing security controls.

HIPAA REGULATORY REFERENCE: 45 CFR 164.308(a)(1)(ii)(A) - **Required specification**
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION: *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (EPHI) held by the covered entity or business associate."*