URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #1B

Title:	**RISK MANAGEMENT**	**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 implementation specification reflects URI's commitment to select and implement security measures to reduce the risks to its information systems containing EPHI to a reasonable and appropriate level.

Specification:

URI must implement security measures that reduce the risks to its information systems containing EPHI to reasonable and appropriate levels. Selection and implementation of such security measures must be based on a formal, documented risk management process.

URI Covered Entities must conduct risk management on a continuous basis and all selected and implemented security measures must ensure the confidentiality, integrity and availability of information systems containing EPHI and be commensurate with the risks to such systems.

Procedure:

1. Security measures must be implemented to reduce the risks to information systems containing EPHI to reasonable and appropriate levels. Selection and implementation of such security measures must be based on a formal, documented risk management process. At a minimum, the risk management process must include the following:

    a. Assessment and prioritization of risks to information systems containing EPHI.
    b. Selection and implementation of reasonable, appropriate and cost-effective security measures to manage, mitigate, or accept identified risks.
    c. Workforce member training and awareness on implemented security measures.
    d. Regular evaluation and revision, as necessary, of existing security measures.

2. URI Covered Entities must manage risk on a continuous basis and all selected and implemented security measures must ensure the confidentiality, integrity and availability of information systems containing EPHI. Strategies for managing risk should be commensurate with the risk prioritization as described below to such

systems, using one or more of the following methods to manage risk: risk acceptance, risk avoidance, risk limitation, or risk transference.

3. URI Covered Entities risk management process must be based on the following steps, which shall be formally documented and securely maintained:

   a. **Inventory -** URI Covered Entities must conduct a regular inventory of its information systems containing EPHI and the security measures protecting those systems. URI Covered Entities must be able to identify its information systems and the relative value and importance of those systems.
   b. **Risk prioritization** - Based on the risks defined by URI Covered Entities risk analysis, risks must be prioritized on a scale from high to low based on the potential impact to information systems containing EPHI and the probability of occurrence. When deciding what URI resources should be allocated to identified risks, highest priority must be given to those risks with unacceptably high-risk rankings.
   c. **Method selection -** URI Covered Entities must select the most appropriate security methods to minimize or eliminate identified risks to information systems containing EPHI. Such selections must be based on the nature of a specific risk and the feasibility and effectiveness of a specific method.
   d. **Security method selection -** URI Covered Entities must determine the most appropriate, reasonable and cost-effective security method(s) for reducing identified risks to information systems containing EPHI.
   e. **Assignment of responsibility** - URI workforce members who have the appropriate expertise must be identified and assigned responsibility for implementing selected security method(s).
   f. **Security method implementation -** Selected security method(s) must be correctly implemented.
   g. **Security method evaluation** - Selected security method(s) must be regularly evaluated and revised as necessary.

HIPAA REGULATORY REFERENCE: 45 CFR 164.308(a)(1)(ii)(B) - **Required specification**
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION*: "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec.164.306 (a)."*