# URI HIPAA SECURITY POLICY #1

| | | | |
|---|---|---|---|
| **Title:** | **SECURITY MANAGEMENT PROCESS** | **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):** | |

## POLICY:

URI Covered Components must ensure the confidentiality, integrity and availability of its information systems containing EPHI by implementing appropriate and reasonable policies, procedures and controls to a) prevent, b) detect, c) mitigate, and d) correct security violations.

URI Covered Components' security management programs must be based on formal and regular processes for risk analysis and management, sanction policies or practices for non-compliance, information system activity review, and training and awareness of workforce members regarding security policies, procedures, and controls.

All URI Covered Component workforce members are responsible for appropriately protecting EPHI maintained on URI information systems from unauthorized access, modification, destruction, and disclosure.

**Procedure**

The following implementation specifications must be followed to satisfy the requirements of this policy:

1. URI Covered Components must regularly identify, define and prioritize risks with respect to the confidentiality, integrity, and availability of its information systems containing EPHI, as specified in URI's **Risk Analysis Implementation Specification (1A)**.

2. URI Covered Components must implement security measures that reduce the risks to its information systems containing EPHI to reasonable and appropriate levels, as specified in URI's **Risk Management Implementation Specification (1B)**.

3. URI Covered Components must apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures, as specified in URI's **Sanction Implementation Specification (1C)**.

4. URI Covered Components must regularly review records of activity on information systems containing EPHI, as specified in the **Information System Activity Review Implementation Specification (1D)**.

**HIPAA REGULATORY INFORMATION**

**CATEGORY:** Administrative Safeguards
**TYPE:** Standard
**HIPAA HEADING:** Security Management Process
**REFERENCE:** 45 CFR 164.308(a)(1)
**SECURITY REGULATION STANDARDS LANGUAGE***: "Implement policies and procedures to prevent, detect, contain and correct security violations."*

**NOTE: REGARDING IMPLEMENTATION AND ENFORCEMENT OF URI HIPAA SECURITY POLICIES AND RELATED IMPLEMENTATION SPECIFICATIONS:**

Unless otherwise specified in the policy or implementation specification, the URI Covered entity management and/or administrator(s) are responsible for monitoring and enforcing the requirements of the policy or specification, in consultation, as needed, with the URI HIPAA Security Officer, and or URI HIPAA Privacy Officer.