URI HIPAA SECURITY POLICY #2

Title:	**ASSIGNED SECURITY RESPONSIBILITY**	**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's Information / HIPAA Security Officer is responsible for the development and implementation of all policies and procedures necessary to appropriately protect the confidentiality, integrity, and availability of EPHI and all URI information systems storing or transmitting EPHI.

Procedure:

The URI Information / HIPAA Security Officer's general work and responsibilities include, but are not limited to:

1. Ensure that URI information systems comply with all applicable federal, state, and local laws and regulations.
2. Ensure that no URI information system compromises the confidentiality, integrity, or availability of any other URI information system.
3. Develop, document, and ensure dissemination of appropriate security policies, procedures, and standards for the users and administrators of URI information systems and the data contained within them.
4. Ensure that newly acquired URI information systems have features that support required and/or addressable security Implementation Specifications.
5. Coordinate the selection, implementation, and administration of significant URI security controls.
6. Ensure URI workforce members receive regular security awareness and training.
7. Conduct periodic risk analysis of URI information systems and security processes.
8. Develop and implement an effective risk management program.
9. Regularly monitor and evaluate threats and risks to URI information systems.
10. Develop and monitor/audit records of URI information systems' activity to identify inappropriate activity.
11. Maintain an inventory of all URI information systems that contain EPHI.
12. Create an effective security incident response policy and related procedures.
13. Ensure adequate physical security controls exist to protect URI's EPHI.
14. Coordinate with URI's Privacy Officer to ensure that security policies, procedures and controls support compliance with the HIPAA Privacy Rule.
15. Evaluate new security technologies that may be appropriate for protecting URI's information systems.

HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: Standard
HIPAA HEADING: Assigned Security Responsibility
REFERENCE: 45 CFR 164.308(a)(2)
SECURITY REGULATION STANDARDS LANGUAGE: "*Identify the security officer who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity".*