URI HIPAA SECURITY POLICY #15

Title:	**AUDIT CONTROLS**	**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 record and examine significant activity on its information systems that contain or use EPHI. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on URI information systems that contain or use EPHI.

PROCEDURE:

The following implementation specifications and safeguards must be implemented to satisfy the requirements of this policy:

1. URI Covered Components must record and examine significant activity on its information systems that contain or use EPHI. URI Covered Components must identify, define, and document what constitutes "significant activity" on a specific information system. Such activity might include:

    - User access to EPHI and user account activity
    - Use of certain software programs or utilities
    - Use of a privileged account
    - Healthcare computing system anomalies, such as unplanned system shutdown or application errors
    - Failed and successful authentication attempts

2. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on URI healthcare systems that contain or use EPHI. At a minimum, such mechanisms must provide the following information:

    - Date and time of activity
    - Origin of activity
    - Identification of user performing activity
    - Description of attempted or completed activity

3. URI Covered Components must develop and implement a standard process for audit log review. At a minimum, the process must include:

    - Definition of which workforce members will review records of activity
    - Definition of what activity is significant
    - Procedures defining how significant activity will be identified and reported

- Procedures for preserving records of significant activity

4. When possible, URI Covered Components workforce members should not review audit logs that pertain to their own system activity. In addition, workforce members should not have the ability to alter or delete log entries that pertain to their own system activity. If it is not possible to limit this access, management should ensure that appropriate compensating controls are documented and implemented.

HIPAA REGULATORY INFORMATION

CATEGORY: Technical Safeguards
TYPE: Standard
HIPAA HEADING: Audit Controls
REFERENCE: 45 CFR 164.312(b)
SECURITY REGULATION STANDARDS LANGUAGE*: "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."*