URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #4B

Title:	**ACCESS ESTABLISHMENT AND MODIFICATION**	**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 have a formal documented process for establishing, documenting, reviewing, and modifying access to URI information systems containing EPHI.

Specification:

URI Covered Entities must have a formal, documented process for establishing, documenting, reviewing, and modifying access to URI information systems containing EPHI.

Authorized URI information system owners/stewards or their designated delegates must regularly review workforce member access rights to URI information systems containing EPHI to ensure that they are provided only to those having a need for specific information in order to accomplish a legitimate task. All revisions to URI workforce member access rights must be tracked and logged.

Procedure:

The following standards and safeguards must be implemented to satisfy the requirements of this standard:

1. URI Covered Entities must have a formal, documented process for establishing, documenting, reviewing, and modifying access to URI information systems containing EPHI. At a minimum, the process must include:

    - Procedure for establishing different levels of access to URI information systems containing EPHI.
    - Procedure for documenting levels of access established to URI information systems containing EPHI.
    - Procedure for regularly reviewing URI workforce member access privileges to URI information systems containing EPHI.
    - Procedure for modifying URI workforce member access privileges to URI information systems containing EPHI.

2. Only properly authorized and trained URI workforce members may access URI information systems containing EPHI. Such access must be established via a formal, documented process. At a minimum, this process must include:

- Identification and definition of permitted access methods
- Identification and definition of length of time that access will be granted
- Procedure for both granting a workforce member an access method (e.g. password or token) and changing an existing access method
- Procedure for managing access rights in a distributed and networked environment
- Appropriate tracking and logging of activities by authorized workforce members on URI information systems containing EPHI

3. Where appropriate, security controls or methods that allow access to be established to URI information systems containing EPHI must include, at a minimum:

    - Unique user identifiers (user IDs) that enable individual users to be uniquely identified. User IDs must not give any indication of the user's privilege level. Common or shared identifiers must not be used to gain access to URI information systems containing EPHI. When unique user identifiers are insufficient or inappropriate, shared identifiers may be used to gain access to URI information systems not containing EPHI. However, this should be a last resort when there are no other feasible alternatives. Further, anytime shared identifiers are used, the system and/or applicable administrators and data owners must have a mechanism of tracking the individuals that are aware of the shared identifiers/credentials. The shared identifiers/credentials must be changed promptly anytime an individual with knowledge of the credentials and passphrase transfers or is terminated from employment by the University, or no longer needs access to the EPHI for any reason.
    - The prompt removal or disabling of access methods for persons and entities that no longer need access to URI EPHI.
    - Verification that redundant user identifiers are not issued.

4. Access to URI information systems containing EPHI must be limited to URI workforce members who have a need for specific EPHI in order to perform their job responsibilities.

5. Appropriate URI information system owners/stewards or their designated delegates must regularly review workforce member access rights to URI information systems containing EPHI to ensure that they are provided only to those who have a need for specific EPHI in order to accomplish a legitimate task. Such rights must be revised as necessary.

6. All revisions to URI workforce member access rights must be tracked and logged. At a minimum, such tracking and logging must provide the following information:
    - Date and time of revision
    - Identification of workforce member whose access is being revised
    - Brief description of revised access right(s)
    - Reason for revision

This information must be securely maintained.

HIPAA REGULATORY REFERENCE: 45 CFR 164.308(a)(4)(ii)(B)
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE*:*
"Implement policies and procedures that, based upon the covered entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."