

URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #10C

Title:	ACCESS CONTROL AND VALIDATION	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 control and validate physical access to its facilities containing healthcare computing systems or software programs that can access healthcare computing systems.

Specification:

URI Covered Entities must control and validate physical access to its facilities that have healthcare computing systems or software programs that can access healthcare computing systems. All physical access rights to such facilities must be clearly defined and documented, with access provided only to URI workforce members who have a need for specific access of the healthcare computing system in order to accomplish a legitimate task. Additionally, such access rights must define specific roles or functions and the physical access rights associated with each.

Procedure:

The following safeguards must be implemented to satisfy the requirements of this implementation specification.

1. URI Covered Entities will identify and document all organizational or functional areas considered sensitive due to the nature of the EPHI that is stored or available within them.
2. After documenting sensitive areas, access rights to such areas should be given only to workforce members who have a need for specific physical access in order to accomplish a legitimate task.
3. All visitors to sensitive facilities where healthcare computing systems are located must show proper identification, state reason for need to access, and sign in prior to gaining access.
4. URI workforce members must immediately report to appropriate management the loss or theft of any device (e.g. card or token) that enables them to gain physical access to such sensitive facilities.
5. URI workforce members must, upon request, present a URI identification badge when at URI facilities where healthcare computing systems are located and should be encouraged to report unknown persons not presenting such identification.

6. All access rights to URI facilities where healthcare computing systems are located or software programs that can access healthcare computing systems must be regularly reviewed and revised as necessary.

HIPAA REGULATORY REFERENCE: 45 CFR 164.310(a)(2)(iii)

HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.”