# URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #3C

| | | | |
|---|---|---|---|
| **Title:** | **TERMINATION PROCEDURES** | **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 create and implement a formal, documented process for terminating access to EPHI when the employment of a workforce member ends.

## Specification:

When the employment of URI Covered Entity workforce members ends, their information systems privileges, both internal and remote, must be disabled or removed by the time of departure. When workforce members depart from URI, they must return all URI supplied equipment by the time of departure. A workforce member who departs from URI must not retain, give away, or remove from URI premises any URI information. Special attention must be paid to situations where a workforce member has been terminated and poses a risk to information or systems at URI.

## Procedure:

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

1. URI Covered Entities must create and implement a formal, documented process for terminating access to EPHI when the employment of a workforce member ends.

2. When the employment of URI Covered Entity workforce members ends, their information systems privileges, both internal and remote, must be disabled or removed by the time of departure. Consideration should also be given to physical access to areas where EPHI is located.

3. All URI Covered Entity workforce members must have their information system privileges automatically disabled after their user ID or access method has had 60 days of inactivity. All such privileges that are disabled in this manner must be reviewed to ensure that the inactivity is not due to termination of employment. If termination is the reason for inactivity, there must be review of situation to ensure that all access to EPHI (or ability to physically access information) has been eliminated.

4. When workforce members depart from URI, they must return all URI supplied equipment (PCs, Tablets, Phones, ID, Keys, etc.) by the time of departure. The return of all such equipment must be tracked and logged

5. If a departing workforce member has used cryptography on URI data, they must make the cryptographic keys available to appropriate management by the time of departure.

6. As appropriate, all physical security access codes used to protect URI information systems that are known by a departing workforce member must be deactivated or changed. For example, the PIN to a keypad lock that restricts entry to an URI facility containing information systems with EPHI must be changed if a workforce member who knows the PIN departs.

7. A workforce member who departs from URI must not retain, give away, or remove from URI premises any URI information (this does not apply to copies of information provided to the public or copies of correspondence directly related to the terms and conditions of employment). All other URI information in the possession of the departing workforce member must be provided to the person's immediate supervisor at the time of departure.

8. Prior to the departure of a terminating URI Covered Entity workforce member, their computers' resident files must be promptly reviewed by their immediate supervisors to determine the appropriate transfer or disposal of any confidential information.

9. Special attention must be paid to situations where a departing employee poses a risk to information or systems at URI. If a workforce member is to be terminated immediately, their information system privileges must be removed or disabled just before they are notified of the termination.

10. URI Covered Entities or their designees must periodically review information system access privileges to ensure that this policy is being adhered to and that existing procedures are effective.

**HIPAA REGULATORY REFERENCE:** 45 CFR 164.308(a)(3)(ii)(C)
**HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE***:*
*"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section."*