URI HIPAA SECURITY POLICY – IMPLEMENATION SPECIFICATION #16A

Title:	**MECHANISM TO AUTHENTICATE ELECTRONIC PROTECTED HEALTH INFORMATION**	**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 implement appropriate electronic mechanisms to confirm that electronic EPHI contained on URI healthcare computing systems has not been altered or destroyed in an unauthorized manner.

Specification:

Where appropriate, URI Covered Entities must implement appropriate electronic mechanisms to confirm that EPHI contained on URI healthcare computing systems has not been altered or destroyed in an unauthorized way.

Procedure:

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

1. Electronic mechanisms used to protect the integrity of EPHI contained on URI healthcare computing systems must ensure that the values and state of the EPHI is maintained, and it is protected from unauthorized modification and destruction. Such mechanisms must also be capable of detecting unauthorized alteration or destruction of EPHI. Such mechanisms might include:

    - System memory, hard drives, and other data storage devices with error-detection capabilities.
    - File and data checksums.
    - Encryption

HIPAA REGULATORY REFERENCE: 45 CFR 164.312(c)(2)
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *"Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner."*