URI HIPAA SECURITY POLICY –
IMPLEMENATION SPECIFICATION #18A

Title:	**INTEGRITY 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):**	

Purpose:

This implementation specification reflects URI's commitment to use appropriate integrity controls to protect the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks.

Specification:

Appropriate integrity controls must be used to protect the confidentiality, integrity, and availability of URI EPHI transmitted over electronic communications networks. URI's integrity controls must ensure that the value and state of all transmitted EPHI is maintained, and the data is protected from unauthorized modification

Procedure:

URI covered components must use integrity controls that are appropriate for protecting the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks. The appropriateness of controls must be based upon sensitivity of and risks to EPHI. For example, EPHI transmitted over public networks represent a much higher risk than EPHI transmitted over URI's campus network. Integrity controls may include, but are not limited to:

- Encryption
- Checksums
- Virtual Private Networks (VPN)

HIPAA REGULATORY REFERENCE: 45 CFR 164.312(e)(2)(i)
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *"Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of."*