URI HIPAA SECURITY POLICY #18

Title:	**TRANSMISSION SECURITY**	**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):**	

POLICY:

This policy reflects URI's commitment to appropriately protect the confidentiality, integrity, and availability of all EPHI that it transmits over electronic communications networks.

PROCEDURE:

1. As defined in URI's **Integrity Controls Implementation Specification (18A)**, URI Covered Components must use integrity controls where appropriate to protect the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks.

2. As defined in URI's **Encryption Implementation Specification (18B)**, URI Covered Components must use encryption where appropriate to protect the confidentiality, integrity, and availability of EPHI transmitted over electronic communications networks.

HIPAA REGULATORY INFORMATION

CATEGORY: Technical Safeguards
TYPE: Standard
HIPAA HEADING: Person or Entity Authentication
REFERENCE: 45 CFR 164.312(d)
SECURITY REGULATION STANDARDS LANGUAGE: *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*