URI HIPAA SECURITY POLICY –
IMPLEMENATION SPECIFICATION #14D

Title:	ENCRYPTION AND DECRYPTION	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 appropriately use encryption to protect the confidentiality, integrity and availability of EPHI contained on URI healthcare computing systems.

Specification:

Where appropriate, encryption should be used to protect the confidentiality, integrity, and availability of EPHI contained on URI Covered Entity computing systems. It is understood that the use of encryption implies that a reliable decryption method is employed.

Procedure:

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

1. URI Covered Entities must consider the following factors at a minimum in determining whether or not specific EPHI must be encrypted on a healthcare computing system:

    *   The sensitivity of the EPHI
    *   The risks to the EPHI
    *   The expected impact to URI functionality and work flow if the EPHI is encrypted
    *   Alternative methods available to protect the confidentiality, integrity, and availability of the EPHI

HIPAA REGULATORY REFERENCE: 45 CFR 164.312(a)(2)(iv)
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *"Implement a mechanism to encrypt and decrypt EPHI."*