URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #1C

Title:	**WORKFORCE SANCTIONS**	**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 apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures.

Specification:

URI's workforce members must comply with all applicable security policies and procedures. URI must have a formal, documented process for applying appropriate sanctions to workforce members who do not comply with its HIPAA / Information security policies and procedures. Sanctions must be commensurate with the severity of the non-compliance with university security policies and procedures

Procedure:

1. URI must have a formal, documented process for applying appropriate sanctions against workforce members who do not comply with its security policies and procedures.

2. The identification and definition of such sanctions are defined in the applicable URI policies to include but are not limited to the URI Acceptable Use Policy and the URI Standard of Conduct of Employees

3. Sanctions can include but are not limited to:

    a. Suspension
    b. Required retraining
    c. Letter of reprimand
    d. Termination

HIPAA REGULATORY REFERENCE: 45 CFR 164.308(a)(1)(ii)(C) – **Required specification**
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."*