URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #5B

Title:	**PROTECTION FROM MALICIOUS SOFTWARE**	**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 provide regular training and awareness to its employees about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems.

Specification:

URI must train Covered Entity workforce members on guarding against, detecting and reporting malicious software that pose a risk to its information systems.

Procedure:

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

1. URI must train workforce members on following procedures for guarding against, detecting and reporting on malicious software.

2. Training and awareness must cover the following topics at a minimum:

    - How to identify and handle potential scams and hoaxes
    - Explanation of how university anti-virus and malware protection software operate
    - How to configure and use anti-virus and mal-ware protection software
    - Good security practices for web browsing, sharing files, and opening email attachments
    - Risks of installing unsupported software
    - Security updates for workstations and software applications
    - What to do when anti-virus and malware protection software detects a virus or a worm.

HIPAA REGULATORY REFERENCE: 45 CFR 164.308(a)(5)(ii)(B)

HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement Procedures for guarding against, detecting, and reporting malicious software…."