URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #5A

Title:	SECURITY REMINDERS	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 security information and awareness to its workforce members.

Specification:

URI must distribute security reminders on a regular basis to its Covered Entity workforce members.

Procedure:

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

1. URI must periodically distribute security reminders to all of its workforce members

2. Security reminders will address security topics that include, but not limited to:

   - Information security policies
   - Information security controls and processes
   - Risks to healthcare information systems and EPHI
     Security best practices (e.g. how to choose a good password, how to report a security incident)
   - URI's information security legal and business responsibilities (e.g. HIPAA, business associate contracts).

3. In addition to providing regular security reminders, URI must provide security information and awareness training all of its workforce members when any of the following events occur:

   - Revision to URI's information security policies and procedures
   - New information security controls are implemented at URI
   - Changes to information security controls
   - Changes in legal or business responsibilities
   - New threats or risks to EPHI

HIPAA REGULATORY REFERENCE: 45 CFR 164.308(a)(5)(ii)(A)
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *“Periodic security updates”*