URI HIPAA SECURITY POLICY –
IMPLEMENTATION SPECIFICATION #7B

Title:	DISASTER RECOVERY PLAN	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 implement a Disaster Recovery Plan to recover its healthcare computing systems if they are impacted by a disaster.

Specification:

URI Covered Entities must create, document, and maintain a Disaster Recovery Plan to recover its information systems if they are impacted by a disaster. URI Covered Entity workforce members with disaster recovery responsibilities must receive annual training on the Disaster Recovery Plan. All appropriate URI workforce members must have access to a current copy of the plan.

Procedure:

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

1. URI Covered Entities must create and document a Disaster Recovery Plan to recover its information systems if they are impacted by a disaster. The plan must be reviewed and revised on an annual basis or more frequently as needed.

2. The Disaster Recovery Plan must include at a minimum:

   - Identification and definition of workforce member responsibilities
   - Conditions for activating the plan
   - Location of data backups
   - Restoration procedures

3. Workforce members with disaster recovery responsibilities must receive annual training on the disaster recovery plan.

4. All appropriate URI workforce members must have access to a current copy of the Disaster Recovery Plan.

HIPAA REGULATORY REFERENCE: 45 CFR 164.308(a)(7)(ii)(B)
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *"Establish (and implement as needed) procedures to restore any loss of data."*