URI HIPAA SECURITY POLICY #7

Title:	**CONTINGENCY 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):**	

POLICY:

URI Covered Components must have an effective process for both preparing for and effectively responding to emergencies and disasters that damage the confidentiality, integrity, or availability of its information systems.

URI's disaster and emergency response process must reduce the disruption to URI information systems to an acceptable level through a combination of preventative and recovery controls and processes. Such controls and processes must identify and reduce risks to URI information systems, limit damage caused by disasters and emergencies, and ensure the timely resumption of significant information systems and processes. Such controls and processes must be commensurate with the value of the information systems being protected or recovered.

URI Covered Component workforce members must receive regular training and awareness on the university's disaster preparation and disaster and emergency response processes.

PROCEDURE:

The following implementation specifications and safeguards must be implemented to satisfy the requirements of this policy:

1. URI Covered Components must have an effective process for assuring all EPHI on the University's information systems and electronic media are regularly backed up and securely stored as specified in URI's **Data Backup Implementation Specification (7A).**
2. URI Covered Components must create and document a Disaster Recovery Plan to recover its information systems if they are impacted by a disaster as specified in URI's **Disaster Recovery Plan Implementation Specification (7B).**
3. URI Covered Components must have an effective Emergency Mode Operations plan to enable the continuance of crucial business processes that protect the security of its information systems containing EPHI during and immediately after a crisis situation as specified in URI's **Emergency Mode Operations Plan Implementation Specification (7C).**
4. URI Covered Components must conduct regular testing of their Disaster Recovery Plan to ensure that it is up to date and effective as specified in URI's **Testing and Revision Procedures Implementation Specification (7D).**
5. URI Covered Components must have an effective process defining and identifying the criticality of its information systems as specified in URI's **Application and Data Criticality Analysis Implementation Specification (7E).**

HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: Standard
HIPAA HEADING: Contingency Plan
REFERENCE: 45 CFR 164.308(a)(7)
SECURITY REGULATION STANDARDS LANGUAGE: *"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."*