URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #13A

Title:	**DISPOSAL**	**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 appropriately dispose of healthcare computing systems and their associated electronic media containing EPHI when it is no longer needed.

Specification:

All URI healthcare computing systems and their associated electronic media containing EPHI that is no longer required must be disposed of in a secure manner. Careless disposal of such information systems and media could result in EPHI being revealed to unauthorized persons. The destruction of any EPHI should be governed by the university's Data Retention Policy or the applicable Covered Entities Data Retention Policy. Questions concerning the destruction of EPHI should be directed to the URI HIPAA Privacy Officer.

Procedure:

1. All URI healthcare computing systems and their associated electronic media containing EPHI must be disposed of properly when no longer needed for legitimate use. The destruction of any EPHI should be governed by the university's Data Retention Policy or the applicable healthcare components' Data Retention Policy. Questions concerning the destruction of EPHI should be directed to the URI HIPAA Privacy Officer. Healthcare computing systems and electronic media to which this policy applies include, but are not limited to: computers (desktops, laptops, phones, tablets, etc.), floppy disks, backup tapes, CD\DVD-ROMs, zip drives, portable hard drives, and flash memory devices.

2. To dispose of a healthcare computing system or electronic medium containing EPHI, the data must be completely removed with data sanitization tool(s) that erase or overwrite media in a manner that prevents the data from being recovered. "Deleting" typically does not destroy data and may enable unauthorized persons to recover EPHI from the media.

3. An alternative to data sanitization of electronic media is physical destruction. The physical destruction of electronic media may be feasible where the media is inexpensive and the destruction methods are easy and safe. For example, floppy disks and CD-ROMs are relatively inexpensive and can be easily destroyed by shredding, if handled carefully.

HIPAA REGULATORY REFERENCE: 45 CFR 164.310(d)(2)(i)

HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored."