URI HIPAA SECURITY POLICY #11

Title:	**WORKSTATION USE**	**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 is to ensure that appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

Workforce members using workstations shall consider the sensitivity of the information, including electronic protected health information (EPHI) that may be accessed and minimize the possibility of unauthorized access.

URI will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Procedure:

The following appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Encrypting Laptops that store or use EPHI.
- Ensuring that security update are being applied for both the operating system and applications.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by using only secure wireless networks.

HIPAA REGULATORY INFORMATION

CATEGORY: Physical Safeguards
TYPE: Standard
HIPAA HEADING: Workstation Use
REFERENCE: 45 CFR 164.310(b)
SECURITY REGULATION STANDARDS LANGUAGE: *"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic protected health information."*