# URI HIPAA SECURITY POLICY #12

| | | | |
|---|---|---|---|
| **Title:** | **WORKSTATION SECURITY** | **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 will prevent unauthorized access to workstations that store or access EPHI while maintaining the access of authorized employees. URI workforce members must not use URI Covered Components workstations to engage in any activity that is either illegal under local, state, federal, or international law, or is in violation of URI policy. Access to URI Covered Component workstations with EPHI must be controlled and authenticated.

## Procedure:

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

1. URI Covered Components must prevent unauthorized physical access to workstations that can access EPHI and ensure that authorized workforce members have appropriate access.

2. All workforce members who use URI Covered Component workstations must take all reasonable precautions to protect the confidentiality, integrity, and availability of EPHI contained on or accessed by the workstations. For example, positioning monitors or shielding workstations so that data shown on the screen is not visible to unauthorized persons.

3. Unauthorized URI Covered Components workforce members must not willfully attempt to gain physical access to workstations that store or access EPHI.

4. URI Covered Component workforce members must report loss or theft of any access device (such as a card or token) that allows them physical access to areas having workstations that can access EPHI.

5. Access to all URI Covered Component workstations must be authenticated via a process that includes, at a minimum:

   - Unique user IDs that enable users to be identified and tracked.
   - Passwords must be masked, suppressed, or otherwise obscured so that unauthorized persons are not able to observe them.
   - The initial password(s) issued to a new URI Covered Components workforce member must be valid only for the new user's first logon to a workstation. At initial logon, the user must be required to choose another password
   - Upon termination of workforce member employment or contracted services, workstation access privileges will be removed.

6. URI Covered Component workforce members must not share their user accounts or passwords with others. If a workforce member believes that someone else is inappropriately using a user account or password, they must immediately notify their manager.

7. Anti-virus software must be installed on workstations to prevent transmission of malicious software. Such software must be regularly updated.

8. URI Covered Component workforce members must activate their workstation locking software whenever they leave their workstation unattended. URI Covered Component workforce members must log off from or lock their workstation(s) when their shifts are complete.

9. Connections from a workstation to a healthcare computing system must be logged off after the session is completed.

10. Special precautions must be taken with portable workstations such as laptops and personal digital assistants (PDA). At a minimum the following guidelines must be followed with such systems:
    - EPHI must not be stored on portable workstations unless such information is appropriately protected. If EPHI is stored on the portable device, it must be encrypted.
    - Locking software for unattended laptops must be activated.
    - Portable workstations containing EPHI must be carried as carry-on (hand) baggage when workforce members use public transport. They must be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile).

11. For workstations with EPHI stored locally on hard drives or other memory devices, additional security measures are required. At a minimum these requirements include:

    - Approval from the URI HIPAA Security Officer must be acquired prior to storing EPHI on workstations or devices external to the Covered Components' existing computer system. URI Covered Components must contact the URI HIPAA Security Officer to identify any database or application that will store electronic protected health information. The HIPAA URI Security Officer will determine if the application or database is legitimate or if it is a duplicate system. If approval is granted, the HIPAA Security Officer will review the security controls against the HIPAA Security requirements.
    - URI Covered Components must inventory and document EPHI stored on workstations when first installed and at least on an annual basis thereafter.
    - URI Covered Components must review and document the security safeguards related to the protection of EPHI stored on their workforce member workstations.
    - Data files containing EPHI will be encrypted wherever possible and password protected.

12. Report theft of all devices to the URI Department of Public Safety immediately.

If the database or application will reside on a portable device, adherence to URI Workstation Security Policy, #0009, and Healthcare Workforce Acceptable Use Policy, #0016, are required.

## HIPAA REGULATORY INFORMATION

**CATEGORY:** Physical Safeguards
**TYPE:** Standard
**HIPAA HEADING:** Workstation Security
**REFERENCE:** 45 CFR 164.310(c)
**SECURITY REGULATION STANDARDS LANGUAGE:** *"Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."*