

**Policy 9**  
**Workstation Use and Security Policy**

Employees are responsible for following the guidelines set forth below when using computer workstations:

- To the extent reasonable, terminal screens should be turned away from visitors and other unauthorized persons or covered with a privacy screen.
- Employees should not eat or drink at their workstation.
- Employees must log off of a workstation if leaving it unattended.
- If employees have portable workstations that contain protected health information (e.g., laptops, smartphones, or tablet type computers), the workstation should be password protected or otherwise kept in a secure manner so that the employee's household members and others do not have access to such workstation.
- Employees are responsible for supervising visitors and patients within the facility – if an unauthorized person is attempting to look at or gain access to a workstation, employees are responsible for informing the visitor or patient that they are not authorized to have access and alerting the Security Officer.
- Employees are responsible for always locking or logging off of their workstation when leaving the workstation unattended. This can be accomplished through using auto-logoff.

## **Explanation of the Workstation Use and Workstation Security Standards and Instructions for Utilizing the Workstation Use and Security Policy**

The Workstation Use Standard and Workstation Security Standard are closely related and, therefore, are addressed together in this explanation and associated policy. Policy 9 is a sample Workstation Use and Security Policy.

### 1. Workstation Use Standard

The Workstation Use Standard requires covered entities to implement policies and procedures specifying the functions that workforce members are permitted to perform on their individual workstations, and the appropriate manner in which these functions should be carried out. Policies and procedures developed pursuant to this standard must also address the physical attributes of the surroundings of workstations with access to electronic protected health information.

Examples of issues that might be addressed in a “Workstation Use” Policy include:

- Employees must logoff of or lock workstations before leaving the workstation unattended
- Employees may not eat or drink while using computer workstations
- Employees should turn computer screens away from visitor areas or utilize privacy screens

### 2. Workstation Security Standard

This standard requires covered entities to implement policies and procedures to limit access to workstations to those individuals who are authorized to use the workstation. The specific measures that will be taken will be dependent on the covered entity’s risk analysis and risk management process. For example, a small provider with a single workstation that is shared by employees with equal access will have fewer issues to address than a large organization with many workstations and varying levels of access.