

Polk County Wisconsin
PHYSICAL SAFEGUARDS
Workstation Security Policy and Procedures
45 CFR §164.310 (c)
REQUIRED

Policy 602.R

Effective Date: October 12, 2004

Revised Date: March 11, 2008

Policy

- A. Polk County Government will implement physical safeguards for all workstations that access electronic protected health information (EPHI) to restrict access to authorized users.
- B. The Information Technology Department will be responsible for implementation of physical safeguards for all workstations that access EPHI to restrict access to authorized users.

Procedures

- A. The Information Technology Department, in coordination with the Department Heads, will be responsible for implementing and monitoring physical safeguards for all workstations that access EPHI to prevent unauthorized access.
- B. Location.
 - 1. Workstations containing EPHI will be located in as secure an environment as possible.
- C. Viewing Procedures.
 - 1. Workstations and other equipment will be positioned in a manner that prevents, to the extent possible, unauthorized viewing of EPHI.
 - 2. Workstations and other equipment will be equipped, to the extent possible, with physical barriers that will restrict viewing to authorized users. (Physical barriers may include antiglare screens, privacy screens or covers that limit viewing.)
- D. Content Review.
 - 1. The content of displays may be reviewed to determine if limiting the content displayed, might better control information access.

- E. Integrity Protection.
 - 1. A virus detection system will be implemented including a process to maintain and update the detection system.
- F. Screen Savers.
 - 1. Screen savers, with password protection, will be installed and utilized with automatic log-offs..
- G. Passwords and Log-ins.
 - 1. Unique password and log-ins will be utilized to control access to the workstation
 - 2. User identification and password authentication mechanisms will be implemented to access the system.
- H. Protection of the EPHI Environment.
 - 1. When appropriate and reasonable, surge protection will be utilized to protect EPHI from power fluctuations.
- I. Other Physical Security Devices.
 - 1. Devices will be used, as appropriate and reasonable, to secure the workstation.
 - 2. Where appropriate and reasonable, restrict removable media to prevent unauthorized copying of EPHI.
 - 3. Software controls that provide for read-only or restricted modification, copying or printing of EPHI.
- J. The Information Technology Department, in coordination with the Privacy Officer and the Department of Employee Relations, will be responsible for documenting, maintaining and retaining information relating to *Policy 602.Q Workstation Security*. The information will be retained for at least six years from the date of creation.

Note: Workstation security is the process of implementing **physical** security controls and practices that will restrict unauthorized access to EPHI. This includes EPHI stored on computer workstations and other equipment such as printers and fax machines.