

**Polk County Wisconsin**  
**PHYSICAL SAFEGUARDS**  
**Workstation Use Policy and Procedures**  
**45 CFR §164.310 (b)**  
**REQUIRED**

**Policy 602.Q**

**Effective Date: October 12, 2004      Revision Date: 3-11-2008**

## **Policy**

- A. Polk County Government will 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 the specific or class of workstation that can access electronic protected health care information (EPHI).
- B. The purpose of the Workstation Use Policy and Procedures is to support the current, or upgraded version of, Polk County Computer Policy and delineate acceptable workstation practices that will protect the confidentiality, integrity and availability of EPHI. The practices should reduce risk of unauthorized access and prevent loss, damage or modification of Polk County Government's EPHI.
- C. The Workstation Use Policy and Procedures apply to all workstations of Polk County Government, including portable and/or remote access workstations.
- D. The Information Technology Department will be responsible, but not limited to development, implementation and monitoring of workstation use policies and procedures.

## **Procedures**

- A. The Information Technology Department will maintain an accurate inventory of workstations, their location and their supervision, including remote access workstations.
- B. The Information Technology Department or other designated person will be responsible for regulating access to workstations. See Access Authorization Policy and Procedures.
- C. The Information Technology Department will be responsible for monitoring compliance with terms and conditions of software licensing and copyright laws.

- D. The Information Technology Department, in coordination with Department Heads, will be responsible for developing and implementing appropriate training relating to workstation use.
- E. The Information Technology Department will implement procedures to monitor the computer system's operating environment.
1. All computer users will monitor their computer system's operating environment and report potential or real threats to the Information Technology Department.
  2. All workstations, if possible, will utilize UPS or surge suppressors in relation to electrical power outlets.
  3. All computer users will comply with the facility's disaster plan and take appropriate measures to protect EPHI.
- F. The Information Technology Department will be responsible for implementing any reasonable methods for maintaining the integrity of EPHI including the use of reasonable and appropriate anti-virus software. The software will be updated weekly, or as needed, to protect the integrity of EPHI.
- G. The Information Technology Department, as reasonable and appropriate, will implement and monitor a password control system on all workstations.
- H. The Information Technology Department, in coordination with Department Heads, as reasonable and appropriate, will regulate and monitor password or other authorized access means to ensure that access is only provided to authorized users.
1. To the extent possible, only unique user identification and log-in identification will provide access.
  2. Workforce members will not share passwords. Workforce members are not allowed to log-in using another workforce member's password or to allow another workforce member to log-in using their password.
  3. Workforce members are not allowed to enter data under another workforce member's password.
  4. Workforce members will not write down their password and leave the password in a publicly accessible location.
  5. Workforce members will make all reasonable attempts to assure that password entry is not observed in a manner that would allow unauthorized access.
  6. Three failed attempts at log-in will result in access denial and notification to the Information Technology Department.

## I. Information Input.

1. Workforce members are responsible for the content of any data the member enters into the computer or transmits through or outside Polk County Government's system.

## J. Workstation Access and Use by Workforce Members.

1. No employee may access any confidential information that is not required to be accessed as a component of their job description or that is authorized by his or her job description or other authorization.
2. No workforce member may download data from Polk County Government's system without explicit authorization from their supervisor, Department Head, or the Information Technology Department.
3. Workforce members will position their monitors to prevent unauthorized access to workstation screens.

## K. Backup.

1. Each computer server will have a backup procedure that will be implemented in compliance with the Data Backup Plan Policy and Procedures.
2. Backup of server data, programs and computer systems will be performed on a regular basis in compliance with the Data Backup Plan Policy and Procedures.

## L. Log-off.

1. Each computer workstation will be programmed with an automatic log-off function that will generate a password-protected screensaver when the computer has not received input for ten minutes.
2. Each user must either lock or log-off the system if they are leaving the computer workstation for more than ten minutes. Explicit reasons must be supplied to supervisor, Department Head, or the Information Technology Department, in order to work around this rule.

## M. Location and Positioning of Workstation Monitors.

1. Workstation monitors will be located in as secure a location as possible.
2. Workstation monitors used infrequently will be located in a secure area or locked when not in use.
3. Workstation monitors will be positioned in a manner that the screens are not readily visible to unauthorized users.
4. Rooms that house workstations containing EPHI that can be locked, will be locked during non-business hours.

#### N. Hard Copy Printouts.

1. The Information Technology Department may assist Department Heads, or supervisors in developing procedures for allowable printing of EPHI.
2. Printed EPHI will be removed from public areas and secured as soon as reasonably possible after printing.
3. Only users that need to print hard copies to perform their job will be allowed to print hard copies of confidential patient information.

O. The Information Technology Department, in coordination with supervisors, or Department Heads will conduct periodic assessments of workstation location, positioning and use.

P. The Information Technology Department, in coordination with the Privacy Officer and the Department of Employee Relations, will be responsible for documentation, maintenance and retention of information relating to Policy 602.Q. Workstation Use. The information will be retained for at least six years from the date of creation.

### **User Responsibilities**

A. Users will attend a Security Awareness and Training Program.

1. Users will sign a statement of understanding relating to requirements of the Security Rule, an agreement to abide by the security requirements and an agreement to protect the confidentiality of EPHI. The agreement to abide by the security requirements includes an obligation to use workstations appropriately. See Policy 601.P Confidentiality
2. Users will be trained in relation to workstation use including the fact that workstations display protected health information and workforce members will be expected to use security precautions that protect the workstation and the workstation display from unauthorized use.

### **Prohibited Workstation Practices**

A. The use of programs or connections to the Internet that may adversely affect confidentiality, integrity or availability of EPHI.

For example: Dissemination of computer viruses, participating in forwarded e-mail that is harassing or offensive, workstation use that is in violation of Polk County Government's privacy, security, or computer policies.

B. Downloading or installing unapproved programs or applications.

C. Unauthorized access to any workstation.

D. Unauthorized use, dissemination or access to EPHI.

E. Refusal to abide by the security requirements of Polk County Government.

**Definition:**

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. [45 CFR 164.304]

