

Health Information Compliance Alert

Security Tool: Stop PHI Violations With A Workstation Security Policy

When securing your organization's computers and the PHI they contain, the best place to start is a no brainer -- your policies.

Use the sample below, provided by information security specialist **Scott Supman**, information security director at **OhioHealth** in Columbus, to develop a policy that will guide your entity down the right security rule path.

PURPOSE:-To eliminate or minimize the possibility of unauthorized access to or contact with protected health-information (PHI).

Workstation Use

1.-Workstation IDs and passwords.

a.-IDs and passwords are required to log onto any workstation that accesses the network. Individuals will authenticate to the network.- For multi-user shared workstations, generic logons are used to access the network, but not the applications.

b.-Initial sign-on passwords expire every 90 days; application-specific passwords expire at least every 90 days.

2. Workstation screen protection.-

a.-If workforce members step away from their workstations, they log off applications completely and invoke a-screensaver lock function.-

b.-[Organization's] workstations automatically invoke a password-protected screensaver timeout after 15 minutes-of inactivity; workstations in areas where the general public might see PHI should invoke the screensaver timeout-after only 1 minute of inactivity.

c.-Once the screensaver is invoked, users must re-authenticate to the network and applications with their user ID-and password.

3.-Workstation logoff.

Where information systems software permits, automatic logout processes are used to terminate-a user's application after a 15-minute period of inactivity. [Organization's] workstations are logged off when not-in use.

Workstation Location

1.-Display screens. All workstations accessing PHI are positioned such that unauthorized personnel cannot readily-view them. Individuals who use transportable workstations are especially aware of screen positioning when the-computer is powered on.

2.-Other. The location of all workstations accessing PHI is reviewed to determine if additional security controls are-needed in addition to the minimum requirements outlined in this policy.

Workstation Monitoring and Review



All workstations and workstation devices are subject to random monitoring at the-direction of information security. Monitoring may include scanning of software, stored data, user activity or any-other scanning required at the discretion of information security. Workstations may be scanned or audited at any-time for any reason.-

Physical Workstation Security and Inventory

- 1.-All workstations are physically secured with anti-theft devices if located in an open office environment.
- 2.-All workstations are formally logged and inventoried.
- 3.-Workstation theft or loss is reported immediately so an incident report can be filed.
- 4.-Workstations at rest are secured with locking cables, placed in locked cabinets or secured via other locking systems.
- 5.-Workstations in an open office environment should not be left unattended unless securely locked.
- 6.-Portable workstations are carried during travel to avoid damage or theft.