



Workstation Use

HIPAA Security ♦ November 2003

Standard Requirement

Workstation use must be addressed as part of the [physical safeguards](#) of the covered entity. This standard requires: “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 a specific workstation or class of workstation that can access [electronic protected health information \(EPHI\)](#).”

Workstation is defined as “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.” ([164.304](#)) Thus PDAs, tablet computers, and other portable/wireless devices are included. DHHS noted specifically in its Final Rule commentary that the standards are not to be interpreted as limited to “fixed location devices.” ([Final Rule, p.8340](#)) The critical variable is not the particulars of the device itself, but whether it can access or store protected health information (PHI). If it can, formal, documented policies and procedures must be in place, and the covered entity must take reasonable, appropriate steps to assure that the policies and procedures are followed.

For a conventional desktop computing device, policies could include requirements to log-off before leaving a workstation unattended or requirements concerning the positioning of the workstation. For a portable device that can leave the covered entity’s premises, policies might restrict the types of information users may enter into the device. The particular rules would be determined by, among other things, results from the covered entity’s risk analysis and risk management efforts, required as part of the [security management process](#) standard.

Covered entities should evaluate threats and vulnerabilities to workstations and to protected health information accessible through the workstation during the risk assessment process. The risk management plan must justify and describe controls instituted to mitigate threats to workstations and associated PHI, including specification of the appropriate physical environment for the workstation. This can be accomplished by addressing the needs of an individual workstation or types of workstations. There are no associated [implementation specifications](#) with this standard.

See also:

[45 CFR 164.310\(b\)](#)

[Device and media controls](#)

Federal and DoD regulations that support this standard

[DoD 8510.1-M](#)

[DoDI 8500.2](#)

PrivacyMail@tma.osd.mil ♦ www.tricare.osd.mil/tmaprivacy