

### 3. Workstation Use (§ 164.310(b))

We proposed policy and guidelines on workstation use that included documented instructions/procedures delineating the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a workstation unattended) to maximize the security of health information. In this final rule, we adopt this standard.

*Comment:* One commenter was concerned most people may be misled by the use of “terminal” as an example in the definition of workstation. The concern was that the standard only addresses “fixed location devices,” while in many instances the workstation has become a laptop computer.

*Response:* For clarity, we have added the definition of “workstation” to § 164.304 and deleted the word “terminal” from the description of workstation use in § 164.310(b).

### 4. Workstation Security (§ 164.310(c))

We proposed that each organization would be required to put in place physical safeguards to restrict access to information. In this final rule, we retain the general requirement for a secure workstation.

*Comment:* Comments were directed toward the example profiled in the definition of a secure workstation location. It was believed that what constitutes a secure workstation location must be dependent upon the entity’s risk management process.

*Response:* We agree that what constitutes an appropriate solution to a covered entity’s workstation security issues is dependent on the entity’s risk analysis and risk management process. Because many commenters incorrectly interpreted the examples as the required and only solution for securing the workstation location, we have modified the regulations text description to generalize the requirement (see § 164.310(c)). Also, for clarity, the title “Secure workstation location” has been changed to “Workstation security” (see also the definition of “Workstation” at § 164.304).

### 5. Device and Media Controls (§ 164.310(d)(1))

We proposed that covered entities have media controls in the form of formal, documented policies and procedures that govern the receipt and removal of hardware and/or software (for example, diskettes and tapes) into and out of a facility. Implementation features would have included “Access control,” “Accountability” (tracking mechanism), “Data backup,” “Data storage,” and “Disposal.”

In this final rule, we adopt most of these provisions as addressable implementation specifications and add a specification for media re-use. We change the name from “Media controls” to “Device and media controls” to more clearly reflect that this standard concerns hardware as well as electronic media. The proposed “Access control” implementation feature has been removed, as it is addressed as part of other standards (see section III.C.12.c of this preamble).

a. *Comment:* One commenter was concerned about the exclusion of removable media devices from examples of physical types of hardware and/or software.

*Response:* The media examples used were not intended to represent all possible physical types of hardware and/or software. Removable media devices, although not specifically listed, are not intended to be excluded.

b. *Comment:* Comments were made that the issue of equipment re-use or recycling of media containing mass storage was not addressed in “Media controls.”

*Response:* We agree that equipment re-use or recycling should be addressed, since this equipment may contain electronic protected health information. The “Device and media controls” standard is accordingly expanded to include a required implementation specification that addresses the re-use of media (see § 164.310(d)(2)(ii)).

c. *Comment:* Several commenters asked for a definition of the term “facility,” as used in the proposed “Media controls” requirement description. Commenters were unclear whether we were talking about a corporate entity or the physical plant.

*Response:* The term “facility” refers to the physical premises and the interior and exterior of a building(s). We have added this definition to § 164.304.

d. *Comment:* Several commenters believe the “Media controls” implementation features are too onerous and should be deleted.

*Response:* While the “Device and media controls” standard must be met, we believe, based upon further review, that implementation of all specifications would not be necessary in every situation, and might even be counter-productive in some situations. For example, small providers would be unlikely to be involved in large-scale moves of equipment that would require systematic tracking, unlike, for example, large health care providers or health plans. We have, therefore, reclassified the “Accountability and data backup” implementation specification as

addressable to provide more flexibility in meeting the standard.

e. *Comment:* One commenter was concerned about the accountability impact of audit trails on system resources and the pace of system services.

*Response:* The proposed audit trail implementation feature appears as the addressable “Accountability” implementation specification. The name change better reflects the purpose and intended scope of the implementation specification. This implementation specification does not address audit trails within systems and/or software. Rather it requires a record of the actions of a person relative to the receipt and removal of hardware and/or software into and out of a facility that are traceable to that person. The impact of maintaining accountability on system resources and services will depend upon the complexity of the mechanism to establish accountability. For example, the appropriate mechanism for a given entity may be manual, such as receipt and removal restricted to specific persons, with logs kept. Maintaining accountability in such a fashion should have a minimal, if any, effect on system resources and services.

f. *Comment:* A commenter was concerned about the resource expenditure (system and fiscal) for total e-mail backup and wanted a clarification of the extensiveness of data backup.

*Response:* The data an entity needs to backup, and which operations should be used to carry out the backup, should be determined by the entity’s risk analysis and risk management process. The data backup plan, which is part of the required contingency plan (see § 164.308(a)(7)(ii)(A)), should define exactly what information is needed to be retrievable to allow the entity to continue business “as usual” in the face of damage or destruction of data, hardware, or software. The extent to which e-mail backup would be needed would be determined through that analysis.

### G. Technical Safeguards (§ 164.312)

We proposed five technical security services requirements with supporting implementation features: Access control; Audit controls; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls;