

3.10 MEDIA PROTECTION

[Quick link to Media Protection Summary Table](#)

MP-1 POLICY AND PROCEDURES

Control:

- a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:
 1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] media protection policy that:
 - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
- b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the media protection policy and procedures; and
- c. Review and update the current media protection:
 1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and
 2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: [PM-9](#), [PS-8](#), [SI-12](#).

Control Enhancements: None.

References: [\[OMB A-130\]](#), [\[SP 800-12\]](#), [\[SP 800-30\]](#), [\[SP 800-39\]](#), [\[SP 800-100\]](#).

MP-2 MEDIA ACCESS

Control: Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

Related Controls: [AC-19](#), [AU-9](#), [CP-2](#), [CP-9](#), [CP-10](#), [MA-5](#), [MP-4](#), [MP-6](#), [PE-2](#), [PE-3](#), [SC-12](#), [SC-13](#), [SC-34](#), [SI-12](#).

Control Enhancements:

(1) MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS

[Withdrawn: Incorporated into [MP-4\(2\)](#).]

(2) MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into [SC-28\(1\)](#).]

References: [\[OMB A-130\]](#), [\[FIPS 199\]](#), [\[SP 800-111\]](#).

MP-3 MEDIA MARKING

Control:

- a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
- b. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].

Discussion: Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Controlled unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in [\[32 CFR 2002\]](#). Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls: [AC-16](#), [CP-9](#), [MP-5](#), [PE-22](#), [SI-12](#).

Control Enhancements: None.

References: [\[EO 13556\]](#), [\[32 CFR 2002\]](#), [\[FIPS 199\]](#).

MP-4 MEDIA STORAGE

Control:

- a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and
- b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Related Controls: [AC-19](#), [CP-2](#), [CP-6](#), [CP-9](#), [CP-10](#), [MP-2](#), [MP-7](#), [PE-3](#), [PL-2](#), [SC-12](#), [SC-13](#), [SC-28](#), [SC-34](#), [SI-12](#).

Control Enhancements:

(1) MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into [SC-28\(1\)](#).]

(2) MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS

Restrict access to media storage areas and log access attempts and access granted using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms include keypads, biometric readers, or card readers on the external entries to media storage areas.

Related Controls: [AC-3](#), [AU-2](#), [AU-6](#), [AU-9](#), [AU-12](#), [PE-3](#).

References: [\[FIPS 199\]](#), [\[SP 800-56A\]](#), [\[SP 800-56B\]](#), [\[SP 800-56C\]](#), [\[SP 800-57-1\]](#), [\[SP 800-57-2\]](#), [\[SP 800-57-3\]](#), [\[SP 800-111\]](#).

[MP-5](#) MEDIA TRANSPORT

Control:

- a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls];
- b. Maintain accountability for system media during transport outside of controlled areas;
- c. Document activities associated with the transport of system media; and
- d. Restrict the activities associated with the transport of system media to authorized personnel.

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic

mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Related Controls: [AC-7](#), [AC-19](#), [CP-2](#), [CP-9](#), [MP-3](#), [MP-4](#), [PE-16](#), [PL-2](#), [SC-12](#), [SC-13](#), [SC-28](#), [SC-34](#).

Control Enhancements:

(1) MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS

[Withdrawn: Incorporated into [MP-5](#).]

(2) MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES

[Withdrawn: Incorporated into [MP-5](#).]

(3) MEDIA TRANSPORT | [CUSTODIANS](#)

Employ an identified custodian during transport of system media outside of controlled areas.

Discussion: Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another if an unambiguous custodian is identified.

Related Controls: None.

(4) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION

[Withdrawn: Incorporated into [SC-28\(1\)](#).]

References: [\[FIPS 199\]](#), [\[SP 800-60-1\]](#), [\[SP 800-60-2\]](#).

[MP-6](#) MEDIA SANITIZATION

Control:

- a. Sanitize [*Assignment: organization-defined system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*]; and
- b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Discussion: Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.

Organizations use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

Related Controls: [AC-3](#), [AC-7](#), [AU-11](#), [MA-2](#), [MA-3](#), [MA-4](#), [MA-5](#), [PM-22](#), [SI-12](#), [SI-18](#), [SI-19](#), [SR-11](#).

Control Enhancements:

(1) MEDIA SANITIZATION | [REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY](#)

Review, approve, track, document, and verify media sanitization and disposal actions.

Discussion: Organizations review and approve media to be sanitized to ensure compliance with records retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.

Related Controls: None.

(2) MEDIA SANITIZATION | [EQUIPMENT TESTING](#)

Test sanitization equipment and procedures [Assignment: organization-defined frequency] to ensure that the intended sanitization is being achieved.

Discussion: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal agencies or external service providers.

Related Controls: None.

(3) MEDIA SANITIZATION | [NONDESTRUCTIVE TECHNIQUES](#)

Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].

Discussion: Portable storage devices include external or removable hard disk drives (e.g., solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

Related Controls: None.

(4) MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION

[Withdrawn: Incorporated into [MP-6](#).]

(5) MEDIA SANITIZATION | CLASSIFIED INFORMATION

[Withdrawn: Incorporated into [MP-6](#).]

(6) MEDIA SANITIZATION | MEDIA DESTRUCTION

[Withdrawn: Incorporated into [MP-6](#).]

(7) MEDIA SANITIZATION | [DUAL AUTHORIZATION](#)

Enforce dual authorization for the sanitization of [Assignment: organization-defined system media].

Discussion: Organizations employ dual authorization to help ensure that system media sanitization cannot occur unless two technically qualified individuals conduct the designated task. Individuals who sanitize system media possess sufficient skills and expertise to determine if the proposed sanitization reflects applicable federal and organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, protecting against errors and false claims of having performed the sanitization actions. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.

Related Controls: [AC-3](#), [MP-2](#).

(8) MEDIA SANITIZATION | [REMOTE PURGING OR WIPING OF INFORMATION](#)

Provide the capability to purge or wipe information from [Assignment: organization-defined systems or system components] [Selection: remotely; under the following conditions: [Assignment: organization-defined conditions]].

Discussion: Remote purging or wiping of information protects information on organizational systems and system components if systems or components are obtained by unauthorized individuals. Remote purge or wipe commands require strong authentication to help mitigate the risk of unauthorized individuals purging or wiping the system, component, or device. The purge or wipe function can be implemented in a variety of ways, including by overwriting data or information multiple times or by destroying the key necessary to decrypt encrypted data.

Related Controls: None.

References: [\[32 CFR 2002\]](#), [\[OMB A-130\]](#), [\[NARA CUI\]](#), [\[FIPS 199\]](#), [\[SP 800-60-1\]](#), [\[SP 800-60-2\]](#), [\[SP 800-88\]](#), [\[SP 800-124\]](#), [\[IR 8023\]](#), [\[NSA MEDIA\]](#).

[MP-7](#) MEDIA USE

Control:

- a. *[Selection: Restrict; Prohibit]* the use of *[Assignment: organization-defined types of system media]* on *[Assignment: organization-defined systems or system components]* using *[Assignment: organization-defined controls]*; and
- b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Discussion: System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to [MP-2](#), which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations use technical and nontechnical controls to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling or removing the ability to insert, read, or

write to such devices. Organizations may also limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

Related Controls: [AC-19](#), [AC-20](#), [PL-4](#), [PM-12](#), [SC-34](#), [SC-41](#).

Control Enhancements:

(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER

[Withdrawn: Incorporated into [MP-7](#).]

(2) MEDIA USE | [PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA](#)

Prohibit the use of sanitization-resistant media in organizational systems.

Discussion: Sanitization resistance refers to how resistant media are to non-destructive sanitization techniques with respect to the capability to purge information from media. Certain types of media do not support sanitization commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media includes compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.

Related Controls: [MP-6](#).

References: [\[FIPS 199\]](#), [\[SP 800-111\]](#).

[MP-8](#) MEDIA DOWNGRADING

Control:

- a. Establish [*Assignment: organization-defined system media downgrading process*] that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information;
- b. Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;
- c. Identify [*Assignment: organization-defined system media requiring downgrading*]; and
- d. Downgrade the identified system media using the established process.

Discussion: Media downgrading applies to digital and non-digital media subject to release outside of the organization, whether the media is considered removable or not. When applied to system media, the downgrading process removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading ensures that empty space on the media is devoid of information.

Related Controls: None.

Control Enhancements:

(1) MEDIA DOWNGRADING | [DOCUMENTATION OF PROCESS](#)

Document system media downgrading actions.

Discussion: Organizations can document the media downgrading process by providing information, such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.

Related Controls: None.

(2) MEDIA DOWNGRADING | [EQUIPMENT TESTING](#)

Test downgrading equipment and procedures [*Assignment: organization-defined frequency*] to ensure that downgrading actions are being achieved.

Discussion: None.

Related Controls: None.

(3) MEDIA DOWNGRADING | [CONTROLLED UNCLASSIFIED INFORMATION](#)

Downgrade system media containing controlled unclassified information prior to public release.

Discussion: The downgrading of controlled unclassified information uses approved sanitization tools, techniques, and procedures.

Related Controls: None.

(4) MEDIA DOWNGRADING | [CLASSIFIED INFORMATION](#)

Downgrade system media containing classified information prior to release to individuals without required access authorizations.

Discussion: Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified systems to unclassified media.

Related Controls: None.

References: [\[32 CFR 2002\]](#), [\[NSA MEDIA\]](#).