

 <b>GEORGIA DEPARTMENT OF COMMUNITY HEALTH</b>		<b>Enterprise Policy</b>	
<b>Policy No.:</b>	<b>539</b>	<b>Division:</b>	<b>Office of Information Technology</b>
<b>Policy Title:</b>	<b>Media Protection (MP)</b>	<b>Effective Date:</b>	<b>December 15, 2025</b>
<b>Version:</b>	<b>3</b>	<b>Category:</b>	<b>Cybersecurity Governance, Risk, and Compliance</b>

### I. Purpose

To properly protect sensitive information from losses due to accidental or intentional misuse of information technology resources, the development, implementation and administration of an overall program management program is critical. This document provides guidance on creating and maintaining this program.

To ensure that the Agency's internal employees, subcontractors and vendors, and anyone with access to sensitive agency information are in compliance with the HIPAA Security Rule and FISMA federal laws through the implementation of the NIST Program Management (PM) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Media Protection (MP) requirements for DCH contractors, business owners, vendors, sponsors, and business partners regarding their roles and responsibilities when access to DCH data and use of applications associated with DCH operations is authorized; and

To reinforce the role of the business owner in providing adequate oversight of contractor responsibilities specific to Program Management obligations outlined in DCH contracts.

### II. Scope

- A.** This document applies to all DCH personnel accessing or utilizing sensitive information in computer resources, data communication networks, or other information technology infrastructure resources owned or leased by DCH, including any other corporation or Agency with connectivity to the network, which is subject to these Information Security Policies.
- B.** This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
- C.** Any personnel found to have violated any agency policy or process shall be subject to sanctions or disciplinary action, up to and including termination of employment.

### III. Policy

- A.** DCH's policy is to implement and manage a formal media protection program that is reviewed and updated at least annually or when circumstances require additional review.

- B.** DCH shall implement and disseminate this policy and procedures to all personnel and contractors.
- C.** DCH shall designate the Chief Information Security Officer (CISO) to manage the development, documentation, implementation, and dissemination of this Media Protection policy and procedures and manage the program.
- D.** In accordance with this policy, DCH shall:
1. Develop, document, implement, manage, and disseminate a comprehensive Media Protection Policy and plan that addresses purpose, scope, roles, and procedures.
  2. Media Classification: DCH categorizes media into the following types, each requiring specific protection measures:
    - Digital Media: Includes all electronic storage devices and mediums, such as: Hard drives, USB flash drives, solid-state drives, CDs, DVDs, and any portable electronic devices (e.g., laptops, tablets, smartphones) digital backup media, such as tapes or cloud-based storage solutions.
    - Non-Digital Media: Includes any physical medium used to store or transmit information, including: Paper documents, blueprints, printouts, medical records, paper-based formats, photographic slides, films, and microfiche.
  3. Restrict access to digital and non-digital media to authorized personnel only.
  4. Mark sensitive media to denote the data classification (e.g., cover sheets stating Confidential for hard copies containing sensitive information).
    - For cases where media cannot be marked due to operational or storage constraints, DCH shall document the justification for the exception and ensure that the media is protected using approved compensating controls consistent with its data classification. Such documentation shall be retained in accordance with the Records Management Policy.
  5. Physically protect both digital and non-digital media.
    - Ensured that digital media is secured until physically destroyed or sanitized (end of life).
    - Deploy protective mechanisms to secure physical media storage areas (e.g., locked rooms, card readers, biometric devices, combination locks, etc.).
    - Non-digital media containing PHI, PII, or other sensitive information shall be stored in locked, access-controlled areas such as secure cabinets or restricted rooms. PHI/PII media must be clearly labeled or otherwise identified to ensure proper handling and storage. If PHI/PII resides on media with mixed-content data, the entire media shall be treated and protected as PHI/PII.
  6. The Media Protection policy and procedures shall be reviewed annually to ensure continued effectiveness, relevance, and compliance with applicable laws, regulations, and industry standards. If necessary, the policy or procedure shall be updated to reflect changes in relevant factors, such as technology, regulations, or internal practices. The revised policy or procedure shall be communicated to all affected parties.
    - Organization-defined events include, but are not limited to, assessment or audit findings; security or privacy incidents; and changes to applicable laws (including privacy laws), Executive Orders, directives, regulations, policies, standards, and guidelines.
  7. Account for movements and transfers of sensitive media by documenting processes and maintaining an updated inventory with locations noted.

- Allow movements and transfers outside of controlled areas to be performed by an authorized designated custodian.
- 8. Utilize approved methods to sanitize and dispose of media commensurate with the classification of the media (data residing in the media) to make the data unrecoverable/unreadable.
  - Document and implement a process to approve media sanitization and disposal, and track and validate that the actions have been performed.
  - Sanitization and disposal records shall include, at minimum: recipient name, signature, media control or serial number, date/time received, routing or chain-of-custody path, media contents, sanitization or destruction method, and date/time completed. These records shall be retained for a minimum of six (6) years or per DCH retention schedules.
  - On a periodic basis, test sanitization methods and procedures to ensure the desired results.
  - DCH shall test all sanitization equipment and tools at least annually to verify they achieve the intended sanitization results. Testing activities and outcomes will be documented and retained according to DCH record retention requirements
  - Provide the capability to perform remote wipes or purging.

## E. Definitions

- DCH – Georgia Department of Community Health
- ePHI - Electronic protected health information or ePHI is defined in HIPAA regulation as any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media. HIPAA regulation states that ePHI includes any of 18 distinct demographics that can be used to identify a patient. See 45 C.F.R. §§ 160.103 and 164.514(b)(2).
- FISMA – Federal Information Security Modernization Act.
- HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law requiring national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
- NIST – The National Institute of Standards and Technology as part of the U.S. Department of Commerce. See <https://www.nist.gov/>.
- PII – Personally Identifiable Information - PII is defined by Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017). PII means information that can be used to distinguish or trace an individual's identity either alone, or when combined with other information that is linked or linkable to a specific individual.
- PHI – Protected Health Information – Individually identifiable health information that is:
  - Transmitted by electronic media
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
  - Excluding individually identifiable health information in:

- Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g;
- Records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
- Employment records held by DCH (a covered entity) in its role as employer; and
- Regarding a person who has been deceased for more than fifty (50) years.
- Sensitive Information - PII, PHI, ePHI, proprietary/trade secret and similar data that require special handling.

**F.** Please refer to NIST 800-53 Media Protection (MP) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Media Protection.



**Signature**

12/18/2025

**Date**

**Revision History**

Version	Date	Description	Author
1.0	11/23/2023	Reviewed and approved by DCH CIO; establishing v1.0	DCH CISO
2.0	11/08/2024	<ul style="list-style-type: none"> <li>• Added a revision history table to validate consistent review/update and document changes</li> <li>• Section D.2: Define the types of digital or non-digital media requiring restricted access</li> <li>• Section D.6: The Media Protection Policy shall be reviewed annually</li> </ul>	DCH CISO
3.0	12/11/2025	<ul style="list-style-type: none"> <li>• Section III.D.6: Change “The Media Protection policy shall be reviewed annually” to “The Media Protection policy and procedures shall be reviewed annually.”</li> <li>• Section III.D.6.1: Updated to define organization-defined events that trigger Media protection policy and procedure review and updates.</li> <li>• Section III.D.4: Added “Updated Media Marking section to clarify documentation requirements for media marking exceptions when marking is not feasible and to allow use of compensating controls consistent with data classification.”</li> <li>• Section III.D.5.3: Added explicit storage and labeling requirements for non-digital PHI/PII and mixed-content media</li> <li>• Section III.D.8.2: Added recordkeeping requirements for sanitization and disposal, including minimum fields and 6-year retention</li> <li>• Section III.D.8.4: Added annual sanitization equipment testing requirement and documentation guidance</li> </ul>	DCH CISO