


| | | | |
|---|--|--------------------------|---|
|  GEORGIA DEPARTMENT OF COMMUNITY HEALTH | | Enterprise Policy | |
| Policy No.: | 533 | Division: | Office of Information Technology |
| Policy Title: | Assessment, Authorization and Monitoring (CA) | Effective Date: | November 26, 2023 |
| Version: | 1 | Category: | Cybersecurity Governance, Risk, and Compliance |

I. Purpose

To properly protect sensitive information from losses due to the accidental or intentional misuse of information technology resources, the development, implementation and administration of an overall Assessment, Authorization and Monitoring 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 comply with the HIPAA Security Rule and FISMA federal laws through the implementation of the NIST Assessment, Authorization and Monitoring (CA) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53.

To establish Assessment, Authorization and Monitoring (CA) 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 Assessment, Authorization and Monitoring (CA) 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 assessment, authorization and monitoring program (Risk Management).
- 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 Systems and Information Integrity policy and procedure and manage the program.
- D.** In accordance with this policy, DCH shall:
 - 1. Require a formal risk assessment performed by an outside independent party who would provide a security assessment report to the state, along with a plan of action and milestone (POAM) report for all identified gaps documented by the accessors.
 - 2. Tracks remediation of POAM gaps along expected remediation timelines to closure.
 - 3. Provide identification and establish a formal function or role for performing control assessments by independent accessor teams.
 - Develop a control assessment plan that identifies the controls under review.
 - Develop assessment procedures, roles, and responsibilities.
 - Review and approve the assessment plan before conducting reviews.
 - Validate that controls are performing as designed and identify any gaps.
 - Provide a formal control assessment report to senior management.
 - 4. Implement security, user, and/or non-disclosure agreements to govern the exchange of information between parties and systems.
 - Each dedicated agreement should have privacy requirements, controls, and responsibilities.
 - All individuals or systems performing the transfers must be explicitly authorized to do so.
 - Discontinue or disallow any information exchanges when the required controls cannot be verified.
 - 5. Develop action plans to remediate or mitigate gaps identified during the control assessment (or other audits, reviews, or monitoring). Action plans shall include milestones, assigned personal and target dates.
 - Deploy the use of automated tools to track, maintain, and validate the accuracy of the action plans.
 - 6. Formally designate an individual responsible for authorizing and deploying system controls and operations. This individual is accountable for managing the overall risk of systems.
 - To further enforce Separation of Duties, designate joint (dual) authorization individuals to perform approvals and authorizations as required.
 - 7. Develop and implement a continuous monitoring strategy to monitor the effectiveness of control assessments and system controls that incorporate risk monitoring for effectiveness, compliance, and change.
 - Monitoring should be performed by independent assessment teams than those performing the assessments or maintaining controls.
 - Identify trends by reviewing information on emerging threats provided by a subscription service.

- Validate that policies and procedures are implemented and operating as intended and in a standardized manner.
- Ensure that monitoring results are accurate and available.
- 8. Perform system penetration testing to identify vulnerabilities on an annual basis.
 - An independent testing team shall perform penetration testing.
 - Utilize red team exercises to simulate adversarial attempts to reveal security vulnerabilities.
 - Utilize testing to bypass or circumvent physical access controls.
- 9. Manage internal system connections by:
 - Authorizing internal connections between system components.
 - Perform security and control checks prior to establishing connections.
 - Documenting for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated.
 - Terminate internal system connections in response to potential security threats or breaches.
 - Review the continued need for each connection periodically.

E. Definition

- Control Assessment - Identification and review of security controls and the effectiveness of the controls in place to address the risks.
- DCH – Georgia Department of Community Health.
- De-Identified – Masking of data to prevent anyone's PII from being identifiable to a specific person.
- 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.
- Information Fragmentation – Threat management technique where information is divided and distributed across multiple systems to reduce the threat of unauthorized access and data exfiltration.
- Least Privilege (Minimum Necessary) – Granting the minimum access needed to perform a specific job role or function.
- 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.
- POAM - Plans of Action and Milestones, or a POAM, is a "document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones", as defined by NIST.
- Role Based Access – Access Group or profile based on defined job functionality within a department or team.
- Sensitive Information - PII, PHI, ePHI, SSA PII, and similar data that require special handling.
- Separation of Duties - Requiring more than one person to complete a task or transaction to prevent one person from controlling every aspect of the process from beginning to end.
- Vulnerability - A security exposure that results from a product weakness that the product developer did not intend to introduce and should fix once it is discovered.

F. References: Please refer to NIST 800-53 Assessment, Authorization and Monitoring (CA) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Awareness and Training.



Signature

November 23, 2023

Date