GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**530**	**Division:**	**Office of Information Technology**
Policy Title:	**Access Control (AC)**	**Effective Date:**	**November 26, 2023**
Version:	**1**	**Category:**	**Cybersecurity Governance, Risk, and Compliance**

I. Purpose

To ensure that the agency's internal employees, subcontractors and vendors, and anyone with access to sensitive information comply with the HIPAA Security Rule and FISMA federal laws through the implementation of the NIST Framework and assist the agency with meeting its FISMA requirements and the current version of NIST 800-53. The term "sensitive" refers to PII, PHI, ePHI, SSA PII, and similar data that require special handling. This document guides the creation and maintenance of this program. It mitigates the risk of threats or incidents involving current or former employees or contractors identified as meeting the High-Risk Insider Threat criteria.

To establish Access Control (AC) 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 Audit and Accountability obligations outlined in DCH contracts. The access privileges of all users, systems, and independently operating programs, such as agents, must be restricted based on "Least Privilege."

II. Scope

A. This policy applies to all DCH personnel (including contractors, vendors, service providers, and business associates) accessing or utilizing computer resources, data communication networks, or other information resources owned or leased by DCH, including any other corporation or agency having connectivity to the network are subject to these Information Security Policies. This policy applies to all who have access to DCH systems but whose access is not specified in a Business Associate Agreement or a Data Use Agreement.

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 information shall be used solely for appropriate agency purposes so that reasonable efforts are made to prevent any use or disclosure of Protected Health Information (PHI) in violation of HIPAA.

B. DCH information shall not be accessed by or disclosed to anyone who does not need the information to perform the activities and fulfill the responsibilities associated with their role.

C. Those authorized to grant or revoke access to DCH information are responsible for following applicable procedures to ensure that access is appropriately assigned, modified as needed, and canceled promptly when individuals transfer to other positions or leave DCH.

D. The State of Georgia recognizes three (3) types of user accounts: Service Account, User Account, and Privileged Account. [Service Accounts can be privileged if technically required, but User Accounts may not. All User Accounts should have a named owner and follow the password policies of the State.

- Service Account – Service Accounts are used to allow system services or applications to connect to a system. These accounts are not intended for individuals to use interactively.
- User Account – User Accounts are designed for use by general users with non-privileged system access.
- Privileged Accounts – Privileged Accounts are users who have the capability to change system configuration settings, grant access, set system controls, or alter system components. They include DBAs, Access Admins, Domain Admins, etc.

D. Those accepting confidential information on behalf of DCH shall ensure that the requirements related to the acceptance of that information are followed.

E. Alleged violations of this policy will be investigated in accordance with the appropriate legal requirements and DCH disciplinary procedures, and when appropriate, sanctions, including, but not limited to dismissal, will be imposed. 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.

F. Unless specifically designated as a public information system, access to any DCH information system network and its resources shall require the use of identification and authentication credentials in accordance with the terms of applicable contracts.

G. All contracts that involve access to DCH systems shall require that DCH's IT Division be notified (per DCH instructions) immediately (and, in no event, more than 1 business day) after any modification or termination of roles. This applies to all DCH business owners, contractors, and vendors.

H. In accordance with this policy, DCH shall:

1. Develop, implement, and provide this Access Control policy to all GA DCH personnel.
2. DCH shall identify the types of allowed and prohibited accounts (e.g., Generic, Operational, Batch Process, API, etc.)
    - The specification shall include each account's authorized users, groups, role members, and access privileges.
    - The parties required to approve access authorizations shall be identified.

- Accounts shall be created, monitored, modified, and disabled in accordance with this policy.
- Account managers shall be notified when accounts are no longer required, or the account owners have terminated them.
- Accounts shall be reviewed to ensure compliance with this policy and be aligned with personnel terminations and transfers.
- Accounts shall be disabled when no longer needed, expired, associated with an individual, inactive, or violating DCH policies.

3. Enforce approved authorization policies and job roles for logical access to information and system resources.
   - Enforce Dual authorization (e.g., two-person control) to reduce the risk of collusion and mitigate the insider threat risk.
   - Enforce mandatory and discretionary access controls to prevent unauthorized access or granting of access or change rule sets.
   - Implement and enforce role-based and attribute (organizational) based access control.
   - Implement a structure for the release of information outside the company.
4. Enforce approved authorizations for controlling the flow of information within and between systems based on Data Classification/Handling and Media Protection requirements.
   - Provide the capability for privileged users to configure security and privacy policies and disable security and privacy filters.
5. Identify and document organizational duties requiring segregation of duties (e.g., submitting and approving an expense report) and define system access authorities in support of separation of duties requirements.
6. Employ the principle of least privilege, allowing only minimum authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. Privileged access should not be assigned to non-organizational users; privileged users should use their non-privileged credentials when accessing non-security functions.
7. Prevent further access to the system by initiating a device lock after a period of inactivity and/or requiring the user to lock their device before leaving the system unattended and retain the device lock until the user identifies themselves and reestablishes authentication.
8. Terminate a user session after a period of inactivity (not terminating a network session). The system shall also display a logout message and when their session will be timed out.
9. Identify all actions that can be performed on the system without identification or authentication (e.g., accessing public websites, receiving faxes) consistent with organizational mission and business functions and document and provide a documented rationale for those.
10. Provide the means to associate [security and privacy attributes] with [security and privacy attribute values] for information in storage, process, and/or transmission. (Note: Security attributes represent the basic properties of active and passive entities concerning safeguarding information.)

11. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed (e.g., teleworking, VPN, wireless) and authorize every kind of remote access to the system before allowing such connections.
12. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access and authorize each type of wireless access (e.g., 802.11x) to the system before allowing such connections.
13. Establish configuration and connection requirements and implementation guidance for organization-controlled mobile devices in alignment with the Mobile Device Policy.
14. Establish the terms and conditions and the controls to be implemented on external systems, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems and upon verification of the external party's controls.
15. Restrict processing and transmitting of organizational information and the use of mobile storage devices on non-organizational systems.
16. Enable authorized users to determine if access authorizations assigned to a sharing partner match the information's access and use restrictions and policies (e.g., Data Classification and/or Information Handling); and employ decision making criteria for sharing or providing access.
17. Designate individuals authorized to make information publicly accessible.
18. Establish procedures or implement mechanisms to ensure user access decisions are applied to each access request before access enforcement.
19. Implement a reference monitor for corporate access control policies that are tamperproof and always invoked to ensure completeness.

IV. Definitions

- Content Filtering - Inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy.
- Data Sanitization - the process of irreversibly removing or destroying data stored on a memory device (e.g., hard drives, flash memory/solid state drives, mobile devices, CDs, and DVDs) or in hard copy form.
- DCH – Georgia Department of Community Health.
- Discretionary Access Control – access controlled by users to their own data.
- 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.

- Least Privilege (Minimum Necessary) – Granting the minimum access needed to perform a specific job role or function.
- Mandatory Access Control – system access control based on security classification.
- NIST - National Institute of Standards and Technology
- 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.
- 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.

V. References: Please refer to NIST 800-53 Access Control Policy (AC) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines, Access Control Policy (PS-08-009).

November 29, 2023

Signature ***Date***