GEORGIA DEPARTMENT OF COMMUNITY HEALTH			Enterprise Policy
Policy No.:	435	Division:	Office of Information Technology
Policy Title:	Managing Authorization, Access, and Control to Information Systems and Request for Network Access	Effective Date:	June 11, 2024
Version:	2.0	Category:	Cybersecurity Governance, Risk, and Compliance

I. Purpose

A. Provide the general framework of the Policy and procedure utilized by the Department of Community Health (DCH) to control access to information and associated applications governing agency operations**.**

B. Clearly document information access control policy and procedures.

C. Avoid the negative consequences that result when information systems are compromised, which consequences may include:

- Sanctions;
- Negative media attention;
- Exposure of personal or private information and subsequent harm to individuals; and
- Unauthorized access to DCH's applications includes unauthorized viewing, modifications, and data copying.

D. Provide for the development of access controls required to protect state and federal information systems.

E. Mitigate the risk of threats or incidents involving current or former employees or contractors who intentionally exceed or misuse an authorized level of access to a network or system or access data in a manner that affects the security of DCH data, systems or daily business operations.

F. Outline managers' responsibilities in managing authorization, access to, and control of DCH's systems and applications as explicitly outlined and agreed to in the DCH Information Technology User Agreement.

G. Establish access control requirements for DCH contractors and business owners, vendors, sponsors, and partners regarding their role and responsibilities when access to DCH data and/or use of applications associated with DCH operations is authorized.

- Reinforce the role of the business owner in providing adequate oversight of contractors' responsibilities specific to access control outlined in DCH contracts.
- Ensure that valid business needs for access associated with DCH assignments continue to exist and that those needs are periodically reviewed and evaluated.

- Assure compliance with all laws that require access controls procedures, including those identified as "References" in the header at the beginning of this document.

II. Scope

A. This Policy establishes requirements for individuals regarding access to all DCH information, including the responsibilities of stewardship and accountability for DCH information needed in carrying out DCH's mission and/or conducting DCH business.

B. This Policy refers to information systems that DCH uses. Access control is required to comply with federal and State regulations and safeguard the confidentiality, integrity, and availability of sensitive and confidential information, including PHI.

C. This Policy describes those procedures necessary for requesting, modifying and deleting user access to systems, applications, and data covered by federal, State, and all other applicable rules and regulations.

D. 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.

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.

- 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 his or her role as stated in Policy 419: DCH IT Use of State Computers.
- 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.
- Those accepting confidential information on behalf of DCH shall ensure that the requirements related to the acceptance of that information are followed.
- Addressing the misuse of Department information and violations of IT Policy 419 is of paramount importance to DCH and will be dealt with on a priority basis. 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.

B. 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 DCH Policies and the terms of applicable contracts.

C. 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.

D. Access authorization shall follow the guidelines established by this Policy and procedure.

E. Access authorization shall be documented, monitored, and managed in accordance with state and DCH guidelines.

F. DCH deploys role-based access control measures based on an individual's role and responsibilities with DCH.

G. The Supervisor/Manager assigns roles based on an employee's organizational function.

H. Supervisors/Managers are responsible for validating and communicating roles and access, where the authorized access level is the lowest level required for users to meet their DCH responsibilities.

I. Upon termination of employment or reassignment of job responsibilities, an employee's user ID and password shall be disabled per the DCH Enterprise Security policy.

J. An employee's access privileges shall be changed accordingly upon reassignment of job responsibilities.

K. In accordance with this Policy, DCH shall:

- Develop, implement, and provide this Access Control policy to all GA DCH personnel.
- 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.

IV. Roles and Responsibilities

A. Georgia Technology Authority (GTA): GTA manages access to the State's technology infrastructure and network services. GTA also controls some applications used by DCH. In addition, GTA manages administrative and physical access to systems. GTA is responsible for all matters related to the State's contracting with outside parties for GETS functions.

B. Georgia Building Authority (GBA) manages the office space occupied by DCH and provides the physical security necessary to provide a secure environment for people, equipment, and information. GBA also manages the Building Access Request System and physical access to the building.

C. DCH Offices, Management, and Staff

1. Commissioner
    i. Leads DCH and conveys the importance of information security to DCH management and staff.
    ii. Supervises the CIO and communicates with other State leaders and the Governor's Office to promote efficient and effective information security measures. The Commissioner has the final authority regarding the granting or termination of information access rights.
2. Chief Information Officer (CIO)
    i. Designates a senior agency information security officer (SAISO) who shall carry out the CIO's responsibilities for information security access control planning and implementation.

ii. Provides guidance and oversight regarding all DCH information security policies, procedures, and access control safeguards to address identity and access management.
iii. Oversees the identification, implementation, and assessment of security access controls throughout DCH's Technology Enterprise.
iv. Ensures that personnel responsible for System, network, and application security access controls are appropriately trained.
v. Assists other senior DCH management with their responsibilities for System, network, and application access security.
vi. Oversees the coordination of cross-platform security access controls for DCH.
vii. Collaborates with the Executive Director of GTA and other State CIO's to address technology and security issues, policies, and standards.

3. Chief Information Security Officer (CISO)
i. Manages information security access control planning and implementation on behalf of the CIO.
ii. Coordinates the development, review, and acceptance of security access controls with IT system owners, access security administration staff, and business owners or authorizing officials.
iii. Coordinates the identification, implementation, and assessment of network, System, and application access security controls.
iv. Plays an active role in developing and updating security access control policies, procedures, and standards and assesses the security impact.
v. Collaborates with the State Chief Information Security Officer and other State agency Information Security Officers to address Enterprise Security Access Control Policies, Procedures, and Standards and their impact on DCH business operations.
vi. Provides oversight and guidance to security administration and operations staff regarding security access control policies, procedures, and standards

4. Access Control Coordinator/Systems Administrator
i. Sets and administers system-wide security controls appropriate for the authority given to users in accordance with the attributes or privileges associated with access control systems.
ii. Acts as the first step of security by creating user IDs and passwords to access the local file servers.
iii. Is appointed by the CIO as the owner and manages the authorized access list.
iv. Acts as the primary point of contact to control settings and coordinate administrative changes for statewide applications, including assigning permission for certain functions and access levels.

5. Inspector General
i. Oversees the criminal background check process for all DCH employees.
ii. Coordinates with the Director of Human Resources to ensure proper background checks for independent contractors and temporary staffing agency employees are complete before access to information systems is granted.
iii. Directs investigations related to violations of DCH information security procedures, including access control procedures, and works with the HIPAA Privacy and Security Officer to recommend sanctions.

iv. Coordinates with the Attorney General and law enforcement when any information security incidents involve criminal behavior.

6. Chief Financial Officer (CFO)

The CFO is the primary authority for DCH staff to access the Financial Systems and related data. The CFO must approve the level of access to the Financial Systems before user IDs and passwords are created.

7. Contracts Administration

i. Is responsible for ensuring that all contracts with business entities that have access to DCH information systems, or that operate information systems on behalf of DCH, includes provisions requiring the maintenance and implementation of acceptable information security controls, including access controls.

ii. Ensures that such contracts incorporate access controls related to DCH information systems and provide penalties for failure to inform DCH of a need for access changes promptly.

8. HIPAA Privacy and Security Officer

i. Works with the CIO, CISO, and Commissioner to revise DCH security controls as needed and ensure proper documentation of DCH policies and procedures.

ii. Works with the CIO, CISO, and Director of Communications to promote compliance with HIPAA security regulations and ensure that all DCH workforce members receive regular security awareness training, including training on access controls.

iii. Works with the Director of Contracts Administration to clarify roles and responsibilities regarding HIPAA security compliance by business associates and develop contract language to address access controls.

iv. Works with the Director of Support Services to promote physical access controls, including the physical security of information systems through worksite audits and support of secure document storage/destruction practices.

v. Works with the Inspector General to investigate violations of DCH information security procedures and recommends sanctions for such violations.

9. Office of Human Resources

i. Is responsible for ensuring that DCH maintains documentation showing that all independent contractors and temporary staffing agency workers have been properly screened in accordance with policies and procedures for background checks.

ii. Maintains documentation that each member of the DCH workforce has access only to those information systems necessary to perform his/her work.

iii. Ensures that all new members of the DCH workforce receive HIPAA Privacy and Security training, which includes training on access restrictions, before receiving access to DCH information systems.

iv. Ensures that all new members of the DCH workforce sign an acknowledgment of the DCH information security procedures.

v. Maintains HIPAA training and acknowledgment forms for DCH employees and ensures that such forms are provided to the HIPAA Privacy and Security Officer for all independent contractors and temporary staffing agency workers.

vi. Ensures that all supervisors are aware of their responsibility to approve information system access only as needed and change the access whenever a staff member's access requirements change.

vii. Ensures that the process for termination of employment includes termination of access to information systems.

10. Support Services

i. Coordinates with GBA and GTA to ensure that physical access to DCH workspace and information systems storage is properly limited through badge access and other controls.

ii. Works with law enforcement to notify DCH staff members of threats to information systems arising from break-ins and thefts.

iii. Coordinates with DCH and other State leaders to ensure that business continuity plans are current and appropriate.

iv. Supports security breach investigations.

11. Director of Vendor and Grantee Management

i. Monitors vendor compliance with information security provisions in service level agreements, including provisions related to access controls.

ii. Is responsible for including information security audits in the vendor management audit process.

12. Director of Procurement/Agency Procurement Officer (APO)

The Director of Procurement/APO is the primary authority for DCH staff to access the PeopleSoft Team Georgia Marketplace (TGM) data. The APO must approve the employee's level of access to the TGM system before a user ID and password are created.

13. System Administrators

i. Are uniquely responsible for enabling users to manage a system or server.

ii. When appropriate, authorize users to define or alter user IDs, set security controls on a system, or alter system components. These higher-level privileges are restricted and controlled and may be extended to performing system support and maintenance activities if not assigned at the enterprise level.

iii. Authorize and manage users' access to with privileges defined by job function and role within DCH.

iv. Serve as the primary business owners for the application/platform system with authorization to perform job functions.

v. Validate privileges annually, report updates to DCH Access Control Coordinator, and perform requested changes to DCH premium networks after obtaining proper authorization.

vi. Retain revalidation results, evidence of completion, and supporting communications for at least 6 years per HIPPA requirements, and define and manage access control requirements, including authorization processes and user ID and password rules for managed applications and systems.

vii. Maintain event/activity logs on all actions for each application under their control.

viii. Are primarily responsible for access to all DCH data closets. Entry for any other staff is strictly prohibited unless an emergency (e.g., fire or water damage) dictates otherwise.

14. Individual Users

i. Defined as any user or network member that requires access to any network, System, or application that accesses, transmits, receives, or stores electronic information.

ii. User IDs for DCH applications shall not be shared, and individual accountability for the security of those IDs must be maintained.

iii. Authorized users are responsible for keeping all account authentication information secure and not permitting any other person to use such accounts for any purpose.

iv. Authorized users shall use all necessary precautions to safeguard the confidentiality of associated passwords and change passwords when directed to comply with scheduled security reviews.

v. Authorized users shall notify the CIO immediately if their password is compromised and is shall not use a password belonging to someone else.

vi. The user is accountable for all activity performed using applicable id's.

vii. Authorized users acknowledge that authorization to use the account will be terminated when they are no longer employees of 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

1. 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.
2. User Account – User Accounts are designed for use by general users with non-privileged system access.
3. Privileged Account – Privileged Accounts enable a user to manage a system or server. They may allow a user to define or alter user id's, set the security controls on the System, or alter system components. Access to Privileged Accounts is not granted to the general user and should be restricted and controlled.

V. Procedure

A. Manager/Supervisor/Business Owner shall:

1. Complete a Request for Network Access to identify an individual DCH user who requires access to the DCH computer system/application.
2. Review the assignment of computer systems annually for employees under his/her direct supervision to ensure that business needs still exist for the specific application.
3. Review access as users change positions or work assignments (e.g., promotion, demotion, transfer, role change, extended leave, or rehire) to ensure that access is maintained or revoked, as appropriate.

B. Access Coordinator/Agency System Administrator shall:

1. Grant access as specified and notify the manager/supervisor/business owner when complete.

2. Forward requests for specific applications to the designated system administrator.
3. Modify or revoke access privileges when users are operating outside their work assignments.
4. Revoke access privileges during a user's extended leave or when deemed appropriate by the Human Resources Office.
5. Request appropriate modification or termination of access privileges to information assets and data systems in accordance with the following:
    a) When the user terminates employment with DCH or the need for access no longer exists, access shall be terminated.
    b) After 60- 90 days of no logon to information systems or applications, access shall be terminated.
    c) When there is unauthorized or wrongful use or disclosure of information, access shall be terminated in accordance with DCH Enterprise Security Policy.
    d) Upon completion of a project or contract work, access shall be terminated and the application administrator shall be notified.

C. Access to Functions

1. Users shall be granted access only to the extent necessary to perform their functions at DCH. Access can be restricted to specific functions within some applications. Access should be as specific and limited as feasible whenever the software allows. Users should only have read or write access to the specific ePHI data required for performing their appropriate function. In most cases, access will fall into one of the following categories:
    a) Administrator/Super-User; or
    b) Regular or Normal User Accounts
2. The minimum access control requirement is a username and a strong password. Every user at DCH must have a unique username. Usernames shall not be shared.
    a) Role-based access may be employed where it improves specificity of access. Role based access allows end-users to access information and resources based on their role within the organization. Role-based access can apply to job categories or to groups of people or individuals.
    b) The use of Anonymous accounts violates this Policy and is strictly prohibited. The use of anonymous user accounts that can access internal agency IT resources, including, but not limited to, PHI, is strictly prohibited unless specifically authorized in writing.
3. If approved by the DCH Information Security Officer and the HIPAA Privacy and Security Officer, DCH may create user accounts for an entity other than DCH that are, In turn, they are authorized to create, modify, and terminate sub-accounts. The security privileges of the user accounts must be approved by the DCH ISO and the HIPAA Privacy and Security Officer. The entities for which the user accounts are created must enter into a written agreement with DCH that describes both the security privileges and the proper use of the accounts. Each such agreement shall set out in specificity the requirements the entity shall follow, which procedures shall be similar to those established by DCH Policy, and to maintain at all times Network Access Control forms approved by DCH, which are substantially similar to the one attached to this Policy. The agreement shall include penalties or other appropriate consequences, as permitted

by law, for failure to promptly terminate access, and shall require the entities to file quarterly updates showing the current users and affirming that their continued use and level of access continues to be appropriate or should be modified.

D. Eligibility for Access

1. Employees whose job responsibilities require access to PHI may be authorized to access specific applications that provide access to PHI, if appropriate, with the written approval of the System Owner and the HIPAA Privacy and Security Officer.
2. Contractors/Temporary Staff providing support to specific DCH functions on a time-limited basis may be authorized access to specific applications for the duration of them Assignments will be done with the written approval of the System Owner.
3. Access shall only be granted to users whose status with DCH is current.
4. Whenever job responsibilities change, the supervisor shall review and determine the appropriate access and request the corresponding changes.
5. If an individual no longer requires access (e.g., upon termination of employment) all access shall be terminated immediately.

E. Access Determination

1. Determining the access to specific applications necessary for job functions and responsibilities require determining which applications are required based on those functions and the corresponding data needed.
2. Every user should be granted the lowest level of access necessary to meet his/ her DCH job responsibilities. This practice is intended to limit the damage that could result from accidents or errors.

F. Monitoring and Oversight

1. The Information Security Officer shall conduct periodic reviews to validate the appropriateness of user accounts and access privileges.
2. Supervisors and System Administrators shall review access requirements annually.
3. Supervisors shall review user access at least twice per year, which reviews can be accomplished during an employee's midyear and annual performance reviews to ensure that each user's access is appropriate.
4. System administrators shall review all user access periodically as a critical function of his/her responsibility to ensure that all users are in current status.
5. All system users consent to such monitoring and accept responsibility for preserving the confidentiality, integrity, and availability of information accessed.

G. Training and Access

1. All DCH employees shall complete HIPAA security training during their new hire orientation and during refresher training as designated by the HIPAA Privacy and Security Officer.
2. Regularly scheduled system activity reviews shall be conducted by the System Administrators to ensure that the level of access to the System is appropriate.

IV. Definitions

- Access Control Coordinator - The authority given to an individual by the assignment of attributes or privileges that are associated with access control systems and that are required for setting and administering system-wide security controls. Individual is designated by the Chief Operating Officer.
- Administrator/Super-User - A special user account used for system administration. Depending on the operating System, the actual name of this account might be: root, administrator or supervisor.
- Agency Procurement Officer (APO) - Primary authority for access to the PeopleSoft Team Georgia Marketplace (TGM) data by DCH staff.
- Contractor An organization or individual that contracts with the Department to supply needed service or skill set. Georgia Building
- Authority (GBA) - The State Authority that manages the property occupied by State agencies and provides the physical security necessary to provide a secure environment for people, equipment and information.
- Georgia Technology Authority (GTA) -The State Authority that establishes information security standards and requirements for the State of Georgia.
- procIT Sabotage Cases in which current or former employees or contractors intentionally exceed or misuse an authorized level of access to networks, systems, or data with the intention of harming a specific individual, the agency, the agency's data, systems, and/or daily operations.
- Privileged Account - Accounts that enable a user to manage a system or server.
- Resource Access Control Facility (RACF) - Designed to provide improved security and controls what users can do on the operating System.
- Security Planning - Requires organizations to have security controls in place or planned for their information systems and the rules of behavior for individuals accessing the information systems.
- Service Account - Used to allow system services or applications to connect to a platform resource.
- Theft Of Information - Cases in which current or former employees or contractors intentionally exceed or misuse an authorized level of access o networks, systems or data with the intention of stealing or orsaiat confidential or proprietary information for the organization.
- Third Parties - Parties who contract with the DCH that administer financial risk to the DCH. User Account Defined as general users with nonprivileged system access.
- User Account – Defined as general users with non-privileged system access.
- 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 USC 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).

June 18, 2024

Signature ***Date***