GEORGIA DEPARTMENT OF COMMUNITY HEALTH			Enterprise Policy
Policy No.:	**536**	**Division:**	**Office of Information Technology**
Policy Title:	**Identification and Authentication (IA)**	**Effective Date:**	**December 18, 2025**
Version:	**3**	**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 Identification and Authentication (IA) 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 comply with the HIPAA Security Rule and FISMA federal laws through the implementation of the NIST Identification and Authentication Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53.

To establish Systems and Identification and Authentication 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 Identification and Authentication 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 Identification and Authentication (IA) program and meet the NIST Digital Identity Guidelines (NIST Special Publication 800-63-3).

B. DCH shall implement and disseminate this policy and procedures to all personnel and contractors.

C. DCH shall designate the Chief Information Security Officer to manage the development, documentation, implementation, and dissemination of the Identification and Authentication procedures in addition to managing the program.

D. In accordance with this policy, DCH shall:

1. Develop, document, implement, manage, and disseminate a comprehensive Identification and Authentication Policy and plan that addresses the purpose, scope, roles, and procedures to implement identification and authentication protocols.
2. Implement a documented methodology to uniquely identify and authenticate all individual users and processes and programs running on behalf of users.
3. Uniquely identify and authenticate all devices before allowing a connection using standardized mechanisms such as Media Access Control (MAC) filtering or 802.1x authentication protocols. A list of approved devices shall be maintained in the System Security and Privacy Plan (SSPP).
    - Standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with DCH requirements.
    - Provide device attestation (identification and authentication) to a device based on its configuration and known operating state.
4. Manage (select and assign) unique system identifiers (e.g., IP Addresses, tokens, MAC addresses) through group, role, service, or device identifier.
5. Do not allow unique identifiers to be reused for a period of two (2) years.
6. Prohibit public identifiers that are readily available (e.g., email addresses) to be used as system account identifiers (e.g., user IDs).
7. All individuals will be managed via a unique identifier (that will not be reassigned or reused and bound to their authentication credentials) in accordance with DCH policies.
8. Ensure unique identifiers explicitly indicate individual user status (e.g., contractors, foreign nationals, non-organizational users) through naming conventions or attribute tags (e.g., appending 'ctr_' to contractor usernames).
9. Provide cross-organization identifier management. (How do you uniquely identify an individual when performing cross-organization tasks?)
10. Maintain the attributes for each uniquely identified individual in a centralized repository (e.g., Active Directory)
11. The Identification and Authentication policy and procedures shall be reviewed annually to ensure their continued effectiveness, relevance, and compliance with applicable laws, regulations, and industry standards. If necessary, the policy and/or procedures shall be updated to reflect changes in relevant factors, such as assessment or audit findings; security or privacy incidents; changes to applicable laws (including privacy laws); Executive Orders, directives, regulations, policies, standards, and guidelines. The revised policy and/or procedures shall be communicated to all affected parties.
12. Manage system authentication by verifying the identity of the individual, group, role, service, or device.

13. Enforce Multi-Factor Authentication (MFA) for all network and local access to privileged and non-privileged accounts. This authentication must utilize at least two different factors to verify the user's identity.
14. Ensure that one of the authentication factors is provided by a device separate from the system gaining access (e.g., a mobile device or hardware token) and meets FIPS 140-2 compliant cryptography standards.
15. Establish a process for initial generation (e.g., automation), authentication distribution (e.g., new user passwords), managing expired or compromised authenticators, and revoking/removing access.
16. Require that the default authenticator (password) is changed before first use.
17. Establish a process for changing authenticators when conditions occur (e.g., lost or compromised password or token).
18. Protect authenticators from unauthorized access or disclosure.
19. Implement replay-resistant authentication mechanisms (e.g., time-based OTPs) for all privileged and non-privileged account access to prevent the unauthorized re-use of valid credentials.
20. Change authenticators when roles or group memberships change. (e.g., badges, tokens, certificates)
21. Maintain a list of commonly used passwords and update the list to include compromised passwords upon discovery.
22. Disallow users from selecting passwords from the database of commonly used passwords.
23. Encrypt transmitted and stored passwords (including application embedded static authenticators).
24. Require immediate password change upon account recovery.
25. Allow long passwords and passphrases for password selection and composition to include all keyboard characters.
26. Enforce password composition and complexity rules, managed via Okta, to include:
27. Minimum password length of eight characters.
28. Complexity requiring at least one uppercase, one lowercase, one numeric, and one special character.
29. Password history retention of 24 generations.
30. Maximum password lifetime of 90 days for user accounts and 45 days for privileged accounts.
31. Case sensitivity enforcement.
32. Support key-based authentication, validate certificates, and utilize an enterprise-wide methodology for using Public Key Infrastructure.
33. Ensure that unique authenticators are in place and default authenticators (e.g., vendor supplied ID passwords) are modified before the system goes live.
34. Protect authenticators commensurate with the system's security classification (e.g., confidential) or information they protect.
35. When possible, require users to utilize different passwords across multiple systems to minimize the risk of a more extensive compromise.
36. Link a person's unique identity and authentication attributes with external providers (e.g., cloud) systems.
37. Avoid the use of Cached Credentials for bypassing network authentication.

38. Implement a documented process for validating the identity of the person being issued the authenticator (e.g., password, token).
39. Obscure authentication credentials on a screen to minimize the opportunity for someone to observe and steal the credentials (e.g., mask passwords, user screen covers, etc.)
40. Implement Cryptographic Module Authentication that meets FIPS 140-2 or higher validation standards to validate a user's identity and verify that the user is authorized to perform a specific function or role.
41. Implement a control to identify and authenticate non-organizational users (e.g., vendors, service providers, etc.). Implement measures to protect the privacy of such individuals (e.g., cryptographic techniques).
42. Identify and validate services (e.g., applications performing queries) before allowing communications or connections to other applications, services, or users.
43. Establish adaptive authentication protocols using pre-established triggers to help assess suspicious behavior, such as excessive login attempts.
44. Require users to re-authenticate following certain events (e.g., session lock, timeout, following role or credential changes).
45. Identity Proof logical access users to Identity Assurance Level 2 (IAL-2) standards as defined in NIST SP 800-63. Identity evidence must be validated and verified through organization-approved methods (e.g., LexisNexis for external users).

E. Definitions

- Cached Credentials – the storage of a user's login credentials/authenticators on a local computer for use when the network authenticator (e.g., Active Directory) is not available.
- Cryptographic Module Authentication – Hardware or Software that supports encryption/decryption functions, digital signatures, and other authentication techniques.
- DCH – Georgia Department of Community Health.
- Encryption**:** Encryption converts electronic data into another form, called ciphertext, which no one except authorized parties can easily understand. Plaintext is what you have before encryption, and ciphertext is the encrypted result.
- Encryption Key: An encryption key is a random string of bits created explicitly for scrambling and unscrambling data. Encryption keys are designed with algorithms to ensure every key is unpredictable and unique. The longer the key is built in this manner, the harder it is to crack the encryption code. An encryption key is used to encrypt, decrypt, or carry out both functions based on the encryption software used.
- 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 – The Federal Information Security Modernization Act of 2014.
- 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.

- Identity Proof - The process of collecting, validating, and verifying a user's identity information to establish system access credentials.
- NIST - The National Institute of Standards and Technology as part of the U.S. Department of Commerce. See https://www.nist.gov/.
- Pairwise pseudonymous identifiers (PPIDs) - An unguessable subscriber identifier generated by an identity provider.
- Password/Passphrase - A string of characters that serve as an authenticator of the user.
- 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, SSA PII, and similar data that require special handling.

F. Please refer to NIST 800-53 Identification and Authentication (IA) and Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for Identification and Authentication.

12/18/2025

Signature ***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	• Added a revision history table to validate consistent review/update and document changes • Section D.5: The Identification and Authentication Policy shall be reviewed annually	DCH CISO
3.0	12/15/2025	• Section III.D.3: Updated to mandate specific device authentication mechanisms (MAC/802.1x) and require an approved device list in the SSPP. • Section III.D.5: Defined a two-year restriction on the reuse of unique identifiers. • Section III.D.7: Added requirement for unique identifiers to explicitly indicate user status through naming conventions. • Section III.D.11: Updated terminology to explicitly reference "policy and procedures" throughout to clarify the full scope of requirements and added specific definitions for factors which influence the policy and procedures revision process. • Section III.D.13: Added requirement to enforce Multi-Factor Authentication (MFA) for all privileged and non-privileged account access. • Section III.D.14: Added requirement for one MFA factor to be a separate, FIPS 140-compliant device. • Section III.D.19: Added requirement for replay-resistant authentication mechanisms, defined password complexity/lifecycle rules managed via Okta, and mandated IAL-2 identity proofing standards per NIST SP 800-63. • Section III.D.40: Updated to mandate FIPS 140-2 or higher validation standards for cryptographic module authentication.	DCH CISO