

 GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Artificial Intelligence (AI) Policy	
Policy No.:	550	Division/Unit:	OIT/Cybersecurity Office
Policy Title:	Artificial Intelligence (AI) Policy	Effective Date:	12/08/2025
Version:	1.0	Category:	Cybersecurity Governance

I. Purpose

The purpose of this policy is to establish requirements for the responsible acquisition, development, deployment, and use of Artificial Intelligence (AI), including Generative AI (GenAI), Machine Learning (ML), and automated decision systems across the Georgia Department of Community Health (DCH). This policy ensures alignment with the State of Georgia's guidance, protects the privacy and security of DCH data, and promotes transparency, accountability, and human oversight across all AI-enabled activities.

II. Scope

- A.** This policy applies to all DCH employees, contractors, vendors, and Third-Party Service Providers (TPSPs) who design, develop, acquire, integrate, configure, manage, access, or use AI systems or AI-enabled functionality on behalf of DCH. This includes AI embedded in SaaS platforms, enterprise applications, cloud services, data analytics tools, or custom solutions supporting DCH programs. It applies to AI tools used for internal operations, administrative processing, cybersecurity, data analytics, case management, decision support, and any automation that uses DCH data or produces outputs influencing DCH decisions.
- 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. Principles:

- **Transparency and Accountability:** AI systems should be designed and used in a way that promotes transparency and accountability.
- **Fairness and Non-Discrimination:** AI systems should be developed and used in a way that is fair and non-discriminatory.
- **Human Oversight:** AI shall support, not replace, human judgment in decision-making, and human oversight should remain central to all AI decision-making processes. A human must review outputs generated by AI before being acted upon for any operational, legal, clinical, financial, or programmatic purpose.

B. Pre-Procurement Review: All AI systems, including GenAI and ML capabilities embedded within enterprise applications, must be reviewed and approved before use. Risk Assessments will be conducted by the DCH Office of Information Security (OIS) to identify and mitigate potential risks associated with AI use. Users must submit proposals for AI-powered software, applications, tools, and services for review before procurement. This review will ensure compliance with established State policies and standards for technology resources, as well as all applicable data protection regulations and guidelines.

C. Documentation and Recordkeeping: DCH will maintain detailed documentation for all AI systems, encompassing:

- System purpose and functionality
- Roles and responsibilities for development, deployment, and oversight
- Training conducted for personnel involved

D. Collaboration Agreements: Collaboration agreements for AI projects must clearly define:

- The manner and purpose of AI use
- Roles, responsibilities, and expectations of all parties involved
- Ownership and usage rights of AI models and data

E. Data Protection: DCH users must adhere to all relevant data protection policies and guidelines, including:

- AI systems must not use, store, share, or process PHI, PII, FTI, SSA data, or HIPAA-regulated data unless contractually authorized and approved by the CISO.
- Training datasets must be documented, auditable, and appropriate for their intended use cases.
- Applying appropriate anonymization, encryption, or other data protection measures.
- Implementing sufficient security measures to safeguard data.
- Obtaining consent from data subjects where necessary.
- Reporting any data breaches or incidents involving AI systems. AI-related security or privacy incidents must follow the DCH Incident Response Plan. Incidents involving the unauthorized use or disclosure of DCH PHI must also be reported to the DCH HIPAA Officer and applicable DCH HIPAA policies and procedures must be followed.
- DCH employees and contractors using AI must complete annual AI awareness training.

F. Annual Review: The Artificial Intelligence policy and supporting procedures shall be reviewed annually to ensure their continued effectiveness, relevance, and compliance with applicable laws, regulations, and industry standards. If necessary, the policy shall be updated to reflect changes in relevant factors, such as technology, regulations, or internal practices. The revised policy shall be communicated to all affected parties.

G. Definitions:

- Artificial Intelligence - A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract these perceptions into models through automated analysis; and use model inference to formulate options for information or action.
- ePHI - Electronic protected health information or ePHI is Protected Health Information (PHI) that is transmitted by electronic media or maintained in electronic media. See the definition at 45 C.F.R. § 160.103.
- Individually Identifiable Health Information – information that is a subset of health information, including demographic information collected from an individual, and is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
 - Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.
 - A covered entity may determine that health information is not individually identifiable health information only if:
 1. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable;
 2. Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
 3. Documents the methods and results of the analysis that justify such determination; or
 4. The identifiers, listed at 45 C.F.R. § 164.514(b)(2)(i), of the individual or of relatives, employers, or household members of the individual, are removed.
- PII – Personally Identifiable Information - PII is defined by the 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 Health Information (SHI): a subset of PHI. Individually identifiable data which indicates sensitive health information including genetic information, substance use disorders, sexually-transmitted diseases and is protected by applicable federal and state laws in addition to HIPAA, such as 42 C.F.R. Part 2 *Confidentiality of Substance Use Disorder Patient Records*.
- Sensitive Information - PII, PHI, ePHI, SSA PII, and similar data that require special handling and may be subject to additional legal protections. Sensitive Information may contain trade secrets or proprietary data, classified data, etc.

G. References: Please refer to:

- [Artificial Intelligence at CMS](#)
- NIST 800-53
- Georgia Technology Authority (GTA) Policy PS-23-001 Enterprise AI Responsible Use



Signature

12/30/2025

Date

Revision History

Version	Date	Description	Author
1.0	12/08/2025	Reviewed and approved by DCH CIO; establishing v1.0	DCH CISO