

 <b>GEORGIA DEPARTMENT OF COMMUNITY HEALTH</b>		<b>Enterprise Policy</b>	
<b>Policy No.:</b>	<b>544</b>	<b>Division:</b>	<b>Office of Information Technology</b>
<b>Policy Title:</b>	<b>Personally Identifiable Information Processing and Transparency (PT)</b>	<b>Effective Date:</b>	<b>December 30, 2025</b>
<b>Version:</b>	<b>3</b>	<b>Category:</b>	<b>Cybersecurity Governance, Risk, and Compliance</b>

## I. Purpose

To properly protect sensitive information from losses due to accidental or intentional misuse of information technology resources, the development, implementation and administration of an overall Personally Identifiable Information Processing and Transparency 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 are in compliance with the HIPAA Security Rule and FISMA federal laws through the implementation of the NIST Personally Identifiable Information Processing and Transparency (PT) Framework and assist the Agency with meeting its FISMA requirements and the current version of NIST 800-53;

To establish Personally Identifiable Information Processing and Transparency 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 Personally Identifiable Information Processing and Transparency obligations outlined in DCH contracts.

## II. Scope

- A.** This document applies to all DCH personnel, subcontractors and vendors, and anyone 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.** It is the policy of DCH to implement and manage a formal Personally Identifiable Information Processing and Transparency program that is reviewed and updated at least annually or when circumstances require additional review.
- 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 Personally Identifiable Information Processing and Transparency policy and procedures in addition to managing the program once the Data Governance Council (DGC) has approved the policy and procedures.
- D.** The Personally Identifiable Information Processing and Transparency policy and procedures shall be reviewed annually to ensure its continued effectiveness, relevance, and compliance with applicable laws, regulations, overarching policy, and industry standards. If necessary, the policy or procedure shall be updated to reflect changes in organization-defined events, including assessment or audit findings; security or privacy incidents; and changes to applicable laws (to include privacy laws), Executive Orders, directives, regulations, policies, standards, and guidelines. The revised policy or procedure shall be communicated to all affected parties.
- E.** DCH shall perform the following:
  - 1. Develop, document, implement, manage, and disseminate a comprehensive Personally Identifiable Information Processing and Transparency policy and plan that addresses purpose, scope, roles, and procedures. Procedures shall include implementation of the PHI and PII processing and transparency policy and the associated PII processing and transparency controls.
  - 2. Through the Data Governance Council (DGC), determine and document which group or role has the authority to permit access to process PII.
    - Restrict access to PII to only those who are authorized to do so.
    - Utilize Data Tags to help identify elements of PII and track and enforce authorized processing of such information.
    - When feasible, manage the enforcement of PII processing through automated tools.
  - 3. Define and implement a mechanism for individuals to provide their consent to have their PII collected and processed, and how that information is to be processed before it is collected.
  - 4. Implement a mechanism to provide notices to individuals as to how their personal information is processed in concise and clear language, to include:
    - Availability to individuals upon first interaction with DCH. The notice shall be provided when the individual first provides the PII.
    - Identification of the authority that approved the processing of PII.
    - Identifies the purpose for which the PII will be processed.
    - Transparency into the information policies and practices with respect to PII.
  - 5. Implement processes to enable individuals to update their personal information that DCH holds to ensure that incorrect and/or outdated information is updated and current.

6. Implement a mechanism that ensures DCH maintains an individual's PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness.
7. DCH shall establish administrative, technical, and physical safeguards to protect PII considering the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
8. DCH shall be accountable for complying with all Fair Information Practice Principles (FIPPs).
9. Establish different categories of PII and processing conditions on each category (e.g., social security numbers (SSNs)). For SSNs:
  - Eliminate unnecessary collection, usage, and storage of SSNs and consider using alternative forms of identification.
  - Inform all individuals whose SSN is requested if the disclosure is voluntary or mandatory, the governing statute, and how the information will be used.

## F. Definitions

- Data Tag – A term assigned to a piece of information that provides a description of the information to aid in the processing.
- DCH – Georgia Department of Community Health
- 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.
- FIPPs – The Fair Information Practice Principles.
  - See <https://www.fpc.gov/resources/fipps/>
- 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.
- NIST – The National Institute of Standards and Technology as part of the U.S. Department of Commerce.
  - See <https://www.nist.gov/>.
- OMB – Office of Management and Budget
- 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, proprietary/trade secret, and similar data that require special handling.

**G.** Please refer to NIST 800-53 Personally Identifiable Information Processing and Transparency (PT) Georgia Technology Authority (GTA) Policies, Standards, and Guidelines for PII Processing and Transparency.



**Signature**

12/31/2025  
**Date**

**Revision History**

Version	Date	Description	Author
1.0	11/23/2023	<ul style="list-style-type: none"> <li>● Reviewed and approved by DCH CIO; establishing v1.0</li> </ul>	DCH CISO
2.0	11/21/2024	<ul style="list-style-type: none"> <li>● Added a revision history table to validate consistent review/update and document changes</li> <li>● Section D: The policy shall be reviewed annually</li> </ul>	DCH CISO
3.0	12/30/2025	<ul style="list-style-type: none"> <li>● Updated version and effective date to the current date.</li> <li>● I – Changed the Program Management program to Personally Identifiable Information Processing and Transparency program,</li> <li>● II. A – extended scope to include subcontractors and vendors, and anyone accessing or utilizing sensitive information, not just DCH employees.</li> <li>● III.D - Added procedure to the section to ensure they are reviewed annually, too.</li> <li>● III.D - Updated section to include Organization-defined events, including assessment or audit findings; security or privacy incidents; and changes to applicable laws (to include privacy laws), Executive Orders, directives, regulations, policies, standards, and guidelines.</li> <li>● III.C - Updated section to state that the Data Governance Council (DGC) must approve any access to PHI/PII.</li> </ul>	DCH CISO

		<ul style="list-style-type: none"> <li>• III.E.2 - Updated section to state that the Data Governance Council (DGC) determines which group, or roles can access PHI/PII.</li> <li>• F – Removed the following items from the glossary that are not used in the document: <ul style="list-style-type: none"> <li>○ Matching Program</li> </ul> </li> <li>• III.E.5 – Added section to ensure individuals can access and amend their PII.</li> <li>• III.E.6 – Added section to ensure DCH maintains the quality and integrity of an individual’s PII.</li> <li>• III.E.7 – Added section to ensure the appropriate security measures are taken with respect to PII, considering risk and magnitude of harm.</li> <li>• III.E.4. bullet 4 – Added bullet to ensure a notice showing transparency into the information policies and practices with respect to PII.</li> <li>• III.E.8 – Added section stating DCH should follow all FIPPs principles.</li> <li>• Added FIPPs to glossary.</li> <li>• Replaces Should with Shall for III.E.7 and III.E.7</li> </ul>	
--	--	--	--