GEORGIA DEPARTMENT OF COMMUNITY HEALTH		Enterprise Policy	
Policy No.:	**544**	**Division:**	**Office of Information Technology**
Policy Title:	**Personally Identifiable Information Processing and Transparency (PT)**	**Effective Date:**	**November 26, 2023**
Version:	**1**	**Category:**	**Cybersecurity Governance, Risk, and Compliance**

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 program management 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 (PT) 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 (PT) 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. It is the policy of DCH to implement and manage a formal Personally Identifiable Information Processing and Transparency (PT) 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.

D. 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. 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 who approved the processing of PII.
    - Identifies the purpose for which the PII will be processed.
5. 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.

E. 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.
- 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.
- Matching Program - a comparison of records from two or more automated systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof).
- 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.

F. 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.

November 23, 2023

Signature ***Date***