PRIVACY POLICY DEFINITIONS

Access: The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.

Access Authorization: The granting of permission in accord with applicable laws for an individual or his/her authorized representative to review and copy any records containing PII or PHI maintained by a Department in accordance with applicable laws.

Access Control: The ability to permit or deny the use of something by someone; a way to protect confidential data on a computer.

Accessibility: The ability to access information and services; the functionality, and possible benefit, of some system or entity.

Availability: Maintaining systems and communications to acceptable operational status.

Business Associate: A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Chief Privacy Officer: An individual who guides and facilitates all ongoing Executive Branch activities related to the development, implementation, maintenance of, and adherence to the applicable laws, policies and procedures governing privacy.

Compliance: Conformity in fulfilling legal or official policy requirements.

Confidential Information: Information that includes, but is not limited to, demographic, medical, and financial information in any form protected by statute or when the release of which would constitute an unreasonable invasion of Privacy, unless the public interest by clear and convincing evidence requires Disclosure in the particular instance, as approved by the designated State

counsel or designee. Confidential Information also includes Personally Identifiable Information (PII), as that term is defined below. Confidential Information may be in paper, electronic and verbal forms, and includes images as well as text. Confidential Information includes all information designated confidential by law, rule, policy or procedure, as may be amended from time to time, such as passwords, client name, trade secrets, information concerning any taxpayer (from any return, declaration, application, audit, investigation, film, record or report) and security audits.

Confidentiality: The assurance that data will only be exposed to those with a lawful right and need to use.

Cookie: Information transmitted from a server to an end-user's web browser, such as Microsoft Internet Explorer, which then re-transmits information back to the server each time the browser accesses a specific server's web page. Cookies usually store information used for authentication, identification or registration of an end-user to a website.

Covered Entity: A (1) health plan, (2) a healthcare clearinghouse, (3) a health care provider who transmits any heath information in electronic form in connection with a transaction covered by HIPAA. A prescription drug card sponsor, an HHS endorsed program, is a covered entity as its operations are considered covered functions which require it to maintain confidentiality of enrollee records in accordance with HIPAA.

Customer: An individual or that individual's authorized representative, or a corporate entity that obtains a product or service from a governmental agency, either voluntarily or involuntarily as may be authorized by law.

De-Identified Health Information: Information that neither identifies nor provides a reasonable basis to identify an individual. Information is de-identified either by a formal determination by a qualified statistician; or the removal of specified identifiers as set forth under HIPAA of the individual, and of his or her relatives, household members and employers, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

Department: A major division of the executive branch of state government that is responsible for administering a specific program area. As used in these policies a department includes its subdivision, bureaus, agencies, boards, commissions, councils, offices and other similarly situated entities.

Designated Record Set: Information recorded in some manner containing information about an individual which is collected for a specific purpose. For those entities covered by HIPAA, a group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;
(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

Disclosure: The release, transfer, provision of access to or divulging or communicating in any other manner of information outside the entity holding the information.

Financial Institution: Under the FTC's Privacy Rule, a financial institution means any institution the business of which is engaging in financial activities as described in § 4(k) of the Bank Holding Company Act of 1956. An entity is not a financial institution unless it is significantly engaged in financial activities.

Incident: Any event that compromises the security, confidentiality, or integrity of PII.

Individual Access: The ability of a person to view the Personally Identifiable Information (PII) maintained about him/her.

Integrity: Keeping data values accurate, and altered only by an authorized person.

Marketing: To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Certain marketing communications are specifically permitted or limited by state and federal law.

Need to Know: The principle that states a user shall only have access to the minimum information necessary to perform a particular function in the exercise of his or her responsibilities.

Non-Public Personal Information (NPPI): NPPI is any personally identifiable information collected about an individual, including but not limited to, social

security numbers, credit card or bank account numbers, medical or educational records, financial information collected by a financial institution used in connection with providing a financial product or service, or other sensitive, confidential or protected data, unless that information is otherwise publicly available.

Opt-In: An approach which requires an individual to affirmatively elect to participate and to agree to the terms of participation by applying to participate.

Opt-out: An approach which assumes that individuals have consented to participate based on their knowledge of the program and failure to object.

Permission: Encompasses both consent and authorization. There will be voluntary agreement (consent) for the initial collection of PII unless the initial collection is required by state or federal law. Subsequent uses and disclosures inconsistent with the permission's scope will require additional consent (authorization). As permitted by law and consistent with Department requirements, consent can be expressed, implied, or provided through an authorized representative. Consent can be given orally, in writing, or electronically consistent with Department requirements.

Personally Identifiable Information or PII: All information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes Protected Health Information (PHI) as that term is defined below. PII is contained in public and non-public records. Examples may include but are not limited to a specific individual's: first name (or initial) and last name (current or former); geographical address; electronic address (including an e-mail address); personal cellular phone number; telephone number or fax number dedicated to contacting the individual at his or her physical place of residence; social security account number; credit and debit card numbers; financial records, including checking, savings and other financial account numbers, and loan accounts and payment history; consumer report information; mother's maiden name; biometric identifiers, including but not limited to, fingerprints, palm prints, facial recognition, full face image and iris scans; driver identification number; birth date; birth, adoption or death certificate numbers; physical description; genetic information; medical, disability or employment records, including salary information; computer information, including information collected through an Internet Cookie; and criminal records and history.. When connected with one or more of the items of information specified above, PII includes any other information concerning an individual that, if disclosed, identifies or can be used to identify a specific individual physically or electronically.

Privacy: The appropriate use and disclosure of PII under the circumstances. What is appropriate will depend on context, law and individual's expectations. Also, the right of an individual to control the collection, use and disclosure of PII.

Privacy Management Team (PMT): The team comprised representatives of Executive Branch department-level organizations established to promote protection of PII (including PHI) while balancing others' need and right to know. The PMT works in collaboration with the Governor's Executive Branch Information Security Team (GEIST) to realize the benefits of information flows within and across agencies, in conformance with privacy policies and laws.

Privacy Notice: Any statement about a Department's privacy and security practices.

Privacy Officer: An individual responsible for implementing privacy policies and procedures of a Department, leading the Department's privacy program and ensuring that the Department complies with its stated procedures.

Protected Health Information or PHI: A subset of PII and means, with regard to HIPAA covered entities (*see* 45 C.F.R. §106.103), individually identifiable health information, including demographic information, whether oral or recorded in any form or medium that relates to an individual's health, health care services and supplies, or payment for services or supplies, and which identifies the individual or could reasonably be used to identify the individual. This includes information that relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual including, but not limited to, preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care as well as counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the body; or the past, present, or future payment for the provision of health care to an individual; and which includes identity information, such as social security number or driver's license number, even if the name is not included, such that the health information is linked to the individual. Protected Health Information does not include records covered by the Family Educational Right and Privacy Act and employment records held by the entity in its role as employer.

Redaction: Permanent removal of sensitive or legally protected information, or PII from paper or digital documents.

Security: The prevention of unauthorized persons from having access to information that is safeguarded.

Security Incident: Any incident that compromises the security, confidentiality, or integrity of PII.

Sensitive PII: Those elements of PII that must receive heightened protection due to legal or policy requirements. Examples of Sensitive PII include, but are not limited to:

i) Social Security numbers
ii) Credit card numbers
iii) Health and Medical data
iv) Driver license numbers
v) Individual financial account numbers

Unauthorized Disclosure: The release of PII that is not authorized by law, policy or the consent of the individual to whom the PII pertains.

- Internal Unauthorized Disclosure: occurs when PII is exposed or potentially exposed to any person(s) within the Department firewall or Department facilities,
- External Unauthorized Disclosure: occurs when PII is exposed or potentially exposed to any person(s) outside the Department firewall or Department facilities.

Use: The access, utilization, employment, application, examination or analysis of information within an entity that maintains such information.

Vendor - An individual or business that may provide commodities and services under contract to governmental entities.

Workforce: Employees, volunteers, trainees and other persons whose conduct, in the performance of work for the State, is under the control of the State, whether or not the State pays them.