CONFIDENTIALITY ACKNOWLEDGEMENT

This Acknowledgement is being instituted to ensure that all Users fully understand their obligations to limit their use of Confidential Information and to protect such information from Unauthorized Disclosure.

NOW, THEREFORE, the User acknowledges and agrees as follows:

1. Definitions:

a. **Confidential Information** means 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. 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 names, trade secrets, information concerning any taxpayer (from any return, declaration, application, audit, investigation, film, record or report) and security audits.

b. **Disclosure** means the release, transfer, provision of access to, sale, divulgence or communication in any other manner of information outside the entity holding the information, in accordance with Policy, as may be amended from time to time.

c. **Need to Know** means 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.

d. **Personally Identifiable Information** or **PII** means 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.

e. **Protected Health Information** or **PHI** is a subset of PII and means**,** with regard to the Health Insurance Portability and Accountability Act of 1996 (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, 20 U.S.C. 1232g, and employment records held by the entity in its role as employer.

f. **Use** means the access, utilization, employment, application, examination or analysis of information within an entity that maintains such information.

g. **User** means employees, volunteers, trainees, and other persons who have access to PHI and PII.

2. Treatment of Confidential Information:

a. The User shall not disclose to anyone, directly or indirectly, any such Confidential Information, unless the individual who is the subject of the Confidential Information consents to the Disclosure in writing or the Disclosure is made pursuant to Policy. At no time shall the Confidential Information be disclosed or used for a personal or non-work-related reason. If information-specific release provisions and restrictions do not exist, then the User shall only disclose Confidential Information (1) upon approval of the designated State counsel or designee; or (2) to individuals who are known by the User to have prior authorization by his or her supervisor to have Access to the information. All of the above applies to release of information in total or fragmented form. When Confidential Information is disclosed, care should be taken to prevent the redisclosure of that information to unauthorized persons or entities. Further, the User shall not misuse any media, documents, forms, or certificates in any manner which might compromise Confidentiality or Security or be otherwise illegal or violate policy, such as altering a record or using a certificate improperly.

b. The User shall protect Confidential Information from unauthorized collection, Use, Access, transfer, sale, Disclosure, alteration, retention or destruction whether accidental or intentional and shall take necessary precautions to secure such Confidential Information to the extent possible.

c. The User is bound by this Agreement and shall continue to protect the Confidential Information to which the User previously had Access, even when he or she no longer has Access to the same.

d. If the User has any questions about this Agreement or the Confidentiality of information or its collection, Use or release, he or she shall request clarification from his or her immediate supervisor or appropriate Privacy Officer at Department of Health and Human Resources.