Protection of Confidential Information*
Standard Language for Personal Service Agreements
9-22-11

***This language replaces the standard language previously required in regard to "Data Encryption"

1) **Put the following in the agreement's definitions section:**

"Confidential Information" shall mean any name, number or other information that may be used, alone or in conjunction with any other information, to identify a specific individual including, but not limited to, such individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation. Without limiting the foregoing, Confidential Information shall also include any information that the Department classifies as "confidential" or "restricted." Confidential Information shall not include information that may be lawfully obtained from publicly available sources or from federal, state, or local government records which are lawfully made available to the general public.

"Confidential Information Breach" shall mean an instance where an unauthorized person or entity accesses Confidential Information in any manner, including but not limited to the following occurrences: (1) any Confidential Information that is not encrypted or protected is misplaced, lost, stolen or in any way compromised; (2) one or more third parties have had access to or taken control or possession of any Confidential Information that is not encrypted or protected without prior written authorization from the State; (3) the unauthorized acquisition of encrypted or protected Confidential Information together with the confidential process or key that is capable of compromising the integrity of the Confidential Information; or (4) if there is a substantial risk of identity theft or fraud to the client, the Contractor, the Department or State.

2) **Replace "Data Encryption" language with the following:**

Protection of Confidential Information

a. Contractor and Contractor Parties, at their own expense, have a duty to and shall protect from a Confidential Information Breach any and all Confidential Information which they come to possess or control, wherever and however stored or maintained, in a commercially reasonable manner in accordance with current industry standards.
b. Each Contractor or Contractor Party shall implement and maintain a comprehensive data - security program for the protection of Confidential Information. The safeguards contained in such program shall be consistent with and comply with the safeguards for protection of Confidential Information, and information of a similar character, as set forth

in all applicable federal and state law and written policy of the Department or State concerning the confidentiality of Confidential Information. Such data-security program shall include, but not be limited to, the following:

1) A security policy for employees related to the storage, access and transportation of data containing Confidential Information;
2) Reasonable restrictions on access to records containing Confidential Information, including access to any locked storage where such records are kept;
3) A process for reviewing policies and security measures at least annually;
4) Creating secure access controls to Confidential Information, including but not limited to passwords; and
5) Encrypting of Confidential Information that is stored on laptops, portable devices or being transmitted electronically.

c. The Contractor and Contractor Parties shall notify the Department and the Connecticut Office of the Attorney General as soon as practical, but no later than twenty-four (24) hours, after they become aware of or suspect that any Confidential Information which Contractor or Contractor Parties possess or control has been subject to a Confidential Information Breach. If a Confidential Information Breach has occurred, the Contractor shall, within three (3) business days after the notification, present a credit monitoring and protection plan to the Commissioner of Administrative Services, the Department and the Connecticut Office of the Attorney General, for review and approval. Such credit monitoring or protection plan shall be made available by the Contractor at its own cost and expense to all individuals affected by the Confidential Information Breach. Such credit monitoring or protection plan shall include, but is not limited to reimbursement for the cost of placing and lifting one (1) security freeze per credit file pursuant to Connecticut General Statutes § 36a-701a. Such credit monitoring or protection plans shall be approved by the State in accordance with this Section and shall cover a length of time commensurate with the circumstances of the Confidential Information Breach. The Contractors' costs and expenses for the credit monitoring and protection plan shall not be recoverable from the Department, any State of Connecticut entity or any affected individuals.

d. The Contractor shall incorporate the requirements of this Section in all subcontracts requiring each Contractor Party to safeguard Confidential Information in the same manner as provided for in this Section.

e. Nothing in this Section shall supersede in any manner Contractor's or Contractor Party's obligations pursuant to HIPAA or the provisions of this Contract concerning the obligations of the Contractor as a Business Associate of the Department.