

Compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations promulgated thereunder:

Except as otherwise limited in this contract, contractor may use or disclose protected health information (PHI) to perform functions, activities, or services for, or on behalf of, the [NAME OF AGENCY] as specified in this contract. In performance of contract services, Contractor agrees to:

- Not use or further disclose protected health information (PHI) other than as permitted or required by the terms of this contract or as required by law;
- Use appropriate safeguards to prevent use or disclosure of PHI other than as permitted by this contract;
- Report to the [NAME OF AGENCY] any use or disclosure of PHI not provided for by this Contract of which it becomes aware;
- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of [NAME OF AGENCY] as required by the HIPAA Security Rule, 45 C.F.R. Parts 160, 162, and 164 and the American Recovery and Reinvestment Act (P.L. 111-5) when effective;
- Ensure that any agent, including a subcontractor, to whom it provides electronic Protected Health Information agrees to implement reasonable and appropriate safeguards to protect it;
- Report to the [NAME OF AGENCY] any security incident of which it becomes aware.
- Contractor shall notify [NAME OF AGENCY] of a breach of unsecured PHI on the first day on which such breach is known by Contractor or an employee, officer or agent of Contractor other than the person committing the breach, or as soon as possible following the first day on which Contractor or an employee, officer or agent of Contractor other than the person committing the breach should have known by exercising reasonable diligence of such breach. Notification shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Contractor to have been, accessed, acquired, used or disclosed during the breach. Contractor shall also provide [NAME OF AGENCY] with any other available information at the time Contractor makes notification to [NAME OF AGENCY] or promptly thereafter as information becomes available. Such additional information shall include (i) a brief description of what happened, including the date of the breach; (ii) a description of the types of unsecured PHI that were involved in the breach; (iii) any steps the Contractor believes individuals should take to protect themselves from potential harm resulting from the breach; and (iv) a brief description of what Contractor is doing to investigate the breach, mitigate harm to individuals, and protect against any future breaches.

For purposes of this paragraph, unsecured PHI means PHI which is not encrypted or destroyed. Breach means the acquisition, access, use or disclosure of PHI in a

manner not permitted by the HIPAA Privacy Rule or this contract which compromises the security or privacy of the PHI by posing a significant risk of financial, reputational, or other harm to the individual.

- Impose the same requirements and restrictions contained in this contract on its subcontractors and agents to whom contractor provides PHI received from, or created or received by a contractor on behalf of the [NAME OF AGENCY];
- Provide access to PHI contained in a designated record set to the [NAME OF AGENCY], in the time and manner designated by the [NAME OF AGENCY], or at the request of the [NAME OF AGENCY], to an individual in order to meet the requirements of 45 CFR 164.524.
- Make available PHI for amendment and incorporate any amendments to PHI in its records at the request of the [NAME OF AGENCY];
- Document and provide to [NAME OF AGENCY] information relating to disclosures of PHI as required for the [NAME OF AGENCY] to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528;
- Make its internal practices, books, and records relating to use and disclosure of PHI received from, or created or received by a contractor on behalf of [NAME OF AGENCY], available to the Secretary of the U.S. Department of Health and Human Services Secretary for the purposes of determining compliance with 45 CFR Parts 160 and 164, subparts A and E;
- At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by a Contractor on behalf of the [NAME OF AGENCY] that the contractor still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

Contractor may use or disclose PHI received from the [NAME OF AGENCY], if necessary, to carry out its legal responsibilities and for the proper management and administration of its business. Contractor may disclose PHI for such purposes if the disclosure is required by law, or if contractor obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially, that it will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and that person will notify the contractor of any instances of which it is aware in which the confidentiality of the information has been breached.