

Executive Order 504 Provider Certification and Data Security Addendum

For all Agreements involving the Provider's access to personal information, as defined in M.G.L. c. 93H, and personal data, as defined in M.G.L. c. 66A, owned or controlled by the Executive Office of Elder Affairs or any other Executive Department agencies, or access to agency systems containing such information or data (herein collectively "personal information"), the Provider certifies under the pains and penalties of perjury that the Provider (1) has read Commonwealth of Massachusetts [Executive Order 504](#) and agrees to protect any and all personal information; and (2) has reviewed all of the [Commonwealth of Massachusetts Information Technology Division's Security Policies](#).

Notwithstanding any contractual provision to the contrary, in connection with the Provider's performance under this Agreement, for all state agencies in the Executive Department, including all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus, and offices, now existing and hereafter established, the Provider shall:

- (1) obtain a copy, review, and comply with the Information Security Program (ISP) of the Executive Office of Elder Affairs upon its release and any pertinent security guidelines, standards and policies and comply with all of the [Commonwealth of Massachusetts Information Technology Division's Security Policies \("Security Policies"\)](#);
- (2) communicate to its workforce the ISP of the Executive Office of Elder Affairs upon its release and such Security Policies and require compliance by all employees (whether such employees are direct or contracted) and subcontractors;
- (3) implement and maintain any other reasonable appropriate security procedures and practices necessary to protect personal information to which the Provider is given access by the Corporation or the Executive Office of Elder Affairs from the unauthorized access, destruction, use, modification, disclosure or loss;
- (4) be responsible for the full or partial breach of any of these terms by its employees (whether such employees are direct or contracted) or subcontractors during or after the term of this Agreement, and any breach of these terms may be regarded as a material breach of this Agreement;
- (5) in the event of any unauthorized access, destruction, use, modification, disclosure or loss of the personal information (collectively referred to as the "unauthorized use"): (a) immediately notify the contracting agency if the Provider becomes aware of the unauthorized use; (b) provide full cooperation and access to information necessary for

the contracting agency to determine the scope of the unauthorized use; and (c) provide full cooperation and access to information necessary for the Corporation, the Executive Office of Elder Affairs and the Provider to fulfill any notification requirements.

(6) comply with all state and federal laws and regulations related to data security, privacy, and confidentiality, including without limitation HIPAA, MGL c. 66A, MGL c. 93H, and (effective January 1, 2010) 201 CMR 17.00 et seq.

Breach of these terms may be regarded as a material breach of this Agreement. In addition, the Provider may be subject to applicable statutory or regulatory penalties, including and without limitation, those imposed pursuant to M.G.L. c. 93H and under M.G.L. c. 214, § 3B for violations under M.G.L. c. 66A.

Provider Name: _____.

Provider Authorized Signature: _____.

Print Name and Title of Authorized
Signatory: _____.

Date: _____.

This Addendum may be signed once and photocopied to be attached to any Provider Agreement and shall be interpreted to be incorporated by reference into any applicable contract or agreement for this Provider.