Business Associate Agreement

This Business Associate Agreement is dated _____, by the **Florida Department of Elder Affairs** (**"Covered Entity"**) and _____, ("**Business Associate**").

1.0 **Background.**

1.1 Business Associate will obtain Protected Health Information from Covered Entity in the performance of one or more contracts or agreements between Covered Entity and Business Associate. Business Associate and subcontractors of Business Associate that provide services in relation to said contracts or agreements are permitted to receive and use protected health information in connection with said contracts or agreements, subject to the terms of this Agreement.

1.2 Covered Entity, recognizes the requirements of the Health Insurance Portability and Accountability Act and has indicated its intent to comply.

1.3 The Health Insurance Portability and Accountability Act regulations establish specific conditions on when and how covered entities may share information with contractors who perform functions for the Covered Entity.

1.4 The Health Insurance Portability and Accountability Act requires the Covered Entity and the Business Associate to enter into a contract or agreement meeting certain standards and containing specific requirements to protect the Confidentiality and Security of patients' protected health information, as set forth in, but not limited to, the Code of Federal Regulations (C.F.R.), specifically 45 C.F.R. §§ 164.502(e), 164.504(e), 164.308(b), and 164.314(a-b)(2013) (as may apply) and contained in this agreement.

1.5 The Health Information Technology for Economic and Clinical Health Act (2009), the American Recovery and Reinvestment Act (2009) and Part I – Improved Privacy Provisions and Security provisions located at 42 United States Code (U.S.C.) §§ 17931 and 17934 (2010), require business associates of covered entities to comply with the Health Insurance Portability and Accountability Act security rule, as set forth in, but not limited to 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316, 45 C.F.R. §164.502(e)(2), and 45 C.F.R. §164.504(e)(2013). Such sections apply to a Business Associate of a Covered Entity in the same manner that such sections apply to the Covered Entity.

The parties therefore agree as follows:

2.0 **Definitions.** For purposes of this agreement, the following definitions apply:

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

2.2 **Administrative Safeguards**. The administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of Security Measures to protect Electronic Protected Health Information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

2.3 **ARRA**. The American Recovery and Reinvestment Act (2009)

2.4 **Authentication**. The corroboration that a person is the one claimed.

2.5 **Availability**. The property of data or information being accessible and useable upon demand by an authorized person.

2.6 **Breach**. The unauthorized or unlawful acquisition, access, use, or disclosure of which Compromises the Security or privacy of such information.

2.7 **Compromises the Security**. Posing a significant risk of financial, reputational, or other harm to individuals.

2.8 **Confidentiality**. The property of data or information being undisclosed and unavailable to unauthorized persons or processes.

2.9 **Designated Record Set**. A group of records maintained by or for a Covered Entity as defined in 45 CFR §164.501.

2.10 **Electronic Protected Health Information. (ePHI)** Individually identifiable health information transmitted by or maintained in electronic media, as specified in 45 C.F.R. §160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

2.11 **HITECH**. The Health Information Technology for Economic and Clinical Health Act (2009)

2.12 **HIPAA.** The Health Insurance Portability and Accountability Act (1996) Pub. L. No. 104-191.

2.13 **Individual**. The person who is the subject of Protected Health Information, as specified in 45 C.F.R. §160.103.

2.14 **Information System**. An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

2.15 **Integrity**. The property of data or information being whole and not altered in an unauthorized manner..

2.16 **Malicious software**. Software, such as a virus, designed to damage or disrupt an electronic Information System.

2.17 **Part I**. Part I – Improved Privacy Provisions and Security provisions located at 42 United States Code (U.S.C.) §§ 17931 and 17934 (2010).

2.18 **Password**. Confidential Authentication information composed of a string of characters.

2.19 **Physical Safeguards**. The physical measures, policies, and procedures to protect a covered entity's electronic Information Systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

2.20 **Privacy Rule**. The Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, subparts A and E.

2.21 **Protected Health Information**. (**PHI)** Health information as defined in 45 C.F.R. §160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

2.22 **Required By Law**. Has the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

2.23 **Secretary**. The Secretary of the Department of Health and Human Services or his or her designee.

2.24 **Security incident**. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System.

2.25 **Security or Security measures**. All of the administrative, physical, and Technical Safeguards in an Information System.

2.26 **Security Rule**. The Security Standards for the protection of Protected Health Information as specified in 45 C.F.R. part 164, subpart C, and amendments thereto.

2.27 **Technical Safeguards**. The technology and the policy and procedures for its use that protect Electronic Protected Health Information and control access to it.

2.28 **Unsecured PHI**. Has the same meaning as the term "Unsecured Protected Health Information" as defined in 45 C.F.R. §164.402.

2.29 All other terms used, but not otherwise defined in this Agreement shall have the same meaning as those terms defined in 45 C.F.R. §§160, 162, and 164, or if not defined therein, the same as the plain meaning of theterm(s).

3.0. **Obligations and Activities of Business Associate.**

3.1 Business Associate agrees to not use or further disclose PHI other than as permitted or required by this agreement or as Required By Law.

3.2 Business Associate agrees to:

(a) Implement policies and procedures to prevent, detect, contain and correct Security violations in accordance with 45 C.F.R. § 164.306;

(b) Prevent use or disclosure of PHI other than as provided for by this Agreement or as Required By Law;

(c) Use appropriate safeguards and comply, where applicable, with Subpart C of 45 C.F.R. §164 with respect to ePHI that the Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity, to prevent use or disclosure of the information other than as provided for by this Agreement or by law; and

(d) Comply with the Security Rule requirements including the Administrative Safeguards, Physical Safeguards, Technical Safeguards, and policies and procedures and documentation requirements set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316, including the provisions of training on such policies and procedures to applicable employees, independent contractors, and volunteers, that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of PHI and/or ePHI that the Provider creates, receives, maintains or transmits on behalf of the Department.

(e) Comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligations, to the extent Business Associate is to carry out Covered Entity's obligations under 45 C.F.R. §164 or this Agreement.

3.3 Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

3.4 Business Associate agrees to report to Covered Entity, without unreasonable delay, any use or disclosure of PHI not provided for by this Agreement of which it becomes aware. This includes any copying or amendment of such information and any Security Breaches involving Unsecured PHI as required by 45 C.F.R. §164.410. Business Associate agrees to include in such notice:

(a) Identification of any individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such Security Breach in accordance with 45 C.F.R. §164.404; and

(b) All information required for the *Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information,* available on the U.S. Department of Health and Human Services website.

3.5 Business Associate agrees to maintain and provide to the Secretary such records and compliance reports as the Secretary may determine to be necessary and to comply with all compliance reviews and complaint investigations as required by the 45 C.F.R. §160, Subsection C.

3.6 Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI that was created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

3.7 If Business Associate has PHI in a Designated Record Set:

(a) Business Associate agrees to provide at the request of Covered Entity during regular business hours, Access to PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an individual in order to meet the requirements under 45 C.F.R. §164.524; and

(b) Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Covered Entity or an Individual within 10 business days of receiving the request.

3.8 Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary upon request from the Secretary for purposes of determining Covered Entity's compliance with the Privacy Rule.

3.9 Business Associate agrees to document such disclosures of PHI and information related thereto as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

3.10 Business Associate agrees to provide to Covered Entity or an Individual, upon request, information collected in accordance with Paragraphs 3.7 and 3.9 above, in response to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §§ 164.528, § 164.502 and § 164.504.

3.11 Business Associate specifically agrees to use Security Measures that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of PHI in electronic or any other form that it creates, receives, maintains, or transmits on behalf of the Covered Entity.

3.12 Business Associate agrees to implement Security Measures to secure Passwords used to Access ePHI that it accesses, maintains, or transmits as part of this Agreement from Malicious Software and other man-made and natural vulnerabilities to assure the Availability, Integrity, and Confidentiality of such information.

3.13 Business Associate agrees to implement Security Measures to safeguard ePHI that it accesses, maintains, or transmits as part of this agreement from Malicious Software and other man-made and natural vulnerabilities to assure the Availability, Integrity, and Confidentiality of such information.

3.14 Business Associate agrees to comply with:

(a) ARRA § 13404 (Application of Knowledge Elements Associated with Contracts), as set forth in 45 C.F.R. §§164.502, 164.504;

(b) ARRA § 13405 (Restrictions on Certain Disclosures and Sales of Health Information), as set forth in 45 C.F.R. §164, Subpart E; and

(c) ARRA § 13406 (Conditions on Certain Contacts as Part of Health Care Operations), as set forth in 45 C.F.R. §§164.508(a)(3), 164.514(f)(1).

4.0 **Permitted Uses and Disclosures by Business Associate**. Except as otherwise limited in this Agreement or any related agreement, Business Associate may use or disclose PHI to perform functions, activities, or services on behalf of Covered Entity**,** provided that such use or disclosure would not violate the Privacy Rule as it applies to Business associate and Covered Entity, or the minimum

necessary policies and procedures of the Covered Entity that are provided to Business Associate by Covered Entity.

5.0 **Specific Use and Disclosure Provisions.**

5.1 Except as otherwise limited in this agreement or any related agreement, Business Associate may use or disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of Business Associate, provided that Business Associate will appropriately safeguard the information in accordance with the Privacy Rule.

5.2 Except as otherwise limited in this agreement or any related agreement, Business Associate may authorize a Business Associate that is a subcontractor to create, receive, maintain or transmit PHI on behalf of Business Associate for the proper management and administration of the Business Associate, provided that Business Associate obtains satisfactory assurances, in accordance with 45 C.F.R. §164.502(e)(1)(ii), and documented in accordance with 45 C.F.R. §164.502(e)(1)(ii)(2), that the subcontractor will appropriately safeguard the information, and, in the event of termination, will return or destroy all PHI and ePHI in accordance with Section 8.3 of this Agreement and 45 C.F.R. §164.504(e)(2)(ii)(J).

5.3 Business Associate may use PHI to provide data aggregation services relating to the health care operations of Covered Entity as permitted by 45 C.F.R. §164.504(e)(2)(i)(B), only when specifically authorized by Covered Entity.

5.4 Business Associate may use or disclose PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. §164.502(j)(1).

6.0 **Obligations of Covered Entity.**

6.1 Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices, to the extent that such limitation may affect Business Associate's use or disclosure of PHI, by providing a copy of the most current Notice of Privacy Practices (NPP) to Business Associate as Attachment I to this Agreement. Future Notices and/or modifications to the NPP shall be posted on Covered Entity's website at www.elderaffairs.state.fl.us.

6.2 Covered Entity shall notify Business Associate of any restriction to the use or disclosure of an Individual's PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

7.0 **Permissible Requests by Covered Entity.** Except for data aggregation or management and administrative activities of Business Associate, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

8.0 **Effective Date and Termination.**

8.1 The Parties hereby agree that this agreement amends, restates and replaces any other Business Associate Agreement currently in effect between Covered Entity and Business Associate and

that the provisions of this agreement shall be effective on the last date that the Agreement has been signed by both parties.

8.2 **Termination for Cause**. Upon Covered Entity's knowledge of a material breach of this agreement or a violation of the Security Rule or the Privacy Rule by Business Associate, Covered Entity shall either:

(a) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(b) Immediately terminate this agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

(c) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

8.3 **Effect of Termination**. Except as provided in subparagraph (b) of this section, upon termination of this agreement, Business Associate shall return or destroy all PHI and ePHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity.

(a) This provision shall apply to PHI and ePHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI and ePHI.

(b) In the event that Business Associate or Covered Entity determines that returning or destroying the PHI or ePHI is infeasible, notification of the conditions that make return or destruction of PHI or ePHI infeasible shall be provided to the other party. Business Associate shall extend the protections of this Agreement to such retained PHI and ePHI and limit further uses and disclosures of such retained PHI and ePHI to those purposes that make the return or destruction of the information infeasible, for a minimum of six years and so long as Business Associate maintains such PHI and ePHI, but no less than six (6) years after the termination of this agreement.

8.4 **Expiration and Effect**. Unless sooner terminated pursuant to Section 8.2 above, this agreement will expire once Business Associate no longer has any PHI in its possession, whether by destruction or return to Covered Entity. Business Associate will provide a certification to Covered Entity once Business Associate no longer has any Data in its possession. Any agreements in place pursuant to Section 3.6 hereof will remain in effect until such agent no longer has any PHI in its possession and certifies same.

9.0 **Regulatory References**. A reference in this agreement to a section in the Privacy Rule or Security Rule means the section then in effect or as may be amended in the future.

10.0 **Amendment.** The Parties agree to take such action as is necessary to amend this agreement as necessary for Covered Entity to comply with the requirements of HIPAA, the Privacy Rule, the Security Rule, and other applicable HIPAA rules.

11.0 **Survival**. Any term, condition, covenant or obligation which requires performance by either party hereto subsequent to the termination of this agreement shall remain enforceable against such party subsequent to such termination.

12.0 **Interpretation**. Any ambiguity in this agreement shall be resolved to permit Covered Entity and Business Associate to comply with 45 C.F.R. §§160, 162, and 164.

13.0 **Incorporation by reference**. Any future new requirement(s), changes or deletion(s) enacted in federal law which create new or different obligations with respect to HIPAA privacy and/or Security, shall be automatically incorporated by reference to this Business Associate Agreement on the respective effective date(s).

14.0 **Notices**. All notices and communications required, necessary or desired to be given pursuant to this agreement, including a change of address for purposes of such notices and communications, shall be in writing and delivered personally to the other party or sent by express 24-hour guaranteed courier or delivery service, or by certified mail of the United States Postal Service, postage prepaid and return receipt requested, addressed to the other party as follows (or to such other place as any party may by notice to the others specify):

To Covered Entity:
Florida Department of Elder Affairs
Attention: «Contract_Manager»
4040 Esplanade Way
Suite «Room»
Tallahassee, Florida 32399

To Business Associate:
_____
Attention: <<_____Director, Legal Affairs>>
_____ADDRESS LINE 1_____
_____ADDRESS LINE 2_____

Any such notice shall be deemed delivered upon actual receipt. If any notice cannot be delivered or delivery thereof is refused, delivery will be deemed to have occurred on the date such delivery was attempted.

15.0 **Governing Law**. The laws of the State of Florida, without giving effect to principles of conflict of laws, govern all matters arising under this agreement.

16.0 **Severability**. If any provision in this agreement is unenforceable to any extent, the remainder of this agreement, or application of that provision to any persons or circumstances other than those as to which it is held unenforceable, will not be affected by that unenforceability and will be enforceable to the fullest extent permitted by law.

17.0 **Successors**. Any successor to Business Associate (whether by direct or indirect or by purchase, merger, consolidation, or otherwise) is required to assume Business Associate's obligations under this agreement and agree to perform them in the same manner and to the same extent that Business Associate would have been required to if that succession had not taken place. This assumption

by the successor of the Business Associate's obligations shall be by written agreement satisfactory to Covered Entity.

18.0 **Entire Agreement**. This agreement constitutes the entire agreement of the parties relating to the subject matter of this agreement and supercedes all other oral or written agreements or policies relating thereto, except that this agreement does not limit the amendment of this agreement in accordance with section 10.0 of this agreement.

Covered Entity: Florida Department of Elder Affairs

By: _____ Date: _____
(signature)
Charles T. Corley, Secretary,
Florida Department of Elder Affairs

Business Associate: _____

By: _____ Date: _____
(signature)
<<_____, Director, Legal Affairs>>