CA-4

ATTACHMENT III
TO
CONTRACT #_____
BUSINESS ASSOCIATE AGREEMENT
BETWEEN
FLORIDA AGENCY FOR PERSONS WITH DISABILITIES ("AGENCY")
AND ("PROVIDER")

This Business Associate Agreement ("Agreement") is made by and between Covered Entity, the Florida Agency for Persons with Disabilities ("Agency" or "Covered Entity") and _____, ("Provider" or "Business Associate") to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), 45 C.F.R. Parts 160, 162, and 164, as well as other applicable federal and state confidentiality laws.

RECITALS

WHEREAS, Business Associate will provide certain services to or on behalf of the Agency. In providing such services under the Contract, Business Associate may receive from the Agency, and may maintain, create, or transmit information on behalf of the Agency that contains protected health information ("PHI") or electronic protected health information ("E-PHI") (both defined below), as collectively referred to herein as "PHI" or "protected health information."

WHEREAS, each party separately acknowledges and agrees that PHI, whether electronic, written, or in oral form shall be safeguarded and any access, use, or disclosure of such information that is created, received, maintained, and/or transmitted between the Agency and the Business Associate, or on behalf of the Agency by Business Associate, shall comply with the requirements of the HIPAA rules.

WHEREAS, the HIPAA rules include but are not limited to requirements that the Agency receive adequate assurances that Business Associate will use appropriate administrative, technical, and physical safeguards to protect the confidentiality of PHI, as shared within the course of providing services to or on behalf of the Agency.

NOW THEREFORE, in consideration of the mutual promises and covenants herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Definitions. The definition of the capitalized terms contained in this Agreement shall have the same meaning and affect as those terms contained in the HIPAA rules, 45 C.F.R. Parts 160, 162, and 164. In the event of any inconsistency between the provisions of

this Agreement and mandatory provisions of the HIPAA rules, the HIPAA rules shall control.

1.1. "Business Associate" has the same meaning as the term "Business Associate" which is defined in 45 C.F.R. § 160.103.

1.2. "Covered Entity" has the same meaning as the term "Covered Entity" which is defined in 45 C.F.R. § 160.103, and in this Agreement means the Florida Agency for Persons with Disabilities ("Agency").

1.3. "HIPAA Rules" means the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), as set forth in 45 C.F.R. Parts 160, 162, and 164.

1.4. "Breach" means the unauthorized acquisition, access, use, or disclosure of PHI under the HIPAA rules which compromises the confidentiality of the PHI. 45 C.F.R. §164.402.

1.5. Protected Health Information or (PHI) shall have the same meaning as such term as defined in 45 C.F.R. § 160.103, but limited to information created, accessed or received by Business Associate on behalf of Covered Entity and also means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium relating to past, present, or future physical or mental health or condition of an individual, provisions of health care to an individual, or the past, present, or future payment for the provisions of health care to an individual. ("Electronic PHI" or "E-PHI" means information transmitted by or maintained in electronic media)

1.6. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. 45 C.F.R. § 164.304.

1.7. "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in the guidance issues under section 13402(h)(2) of Public Law 111-5. 45 C.F.R. § 164.402.

2. Purposes for which PHI May Be Disclosed to Business Associate. In connection with the services provided by Business Associate to or on behalf of the Agency, the Agency shall only disclose PHI to Business Associate for the stated purposes referenced in Contract #_____ and shall limit disclosure to the minimum necessary information to accomplish the intended purpose referenced Contract #_____.

3. Disclosure to Third Parties, Agents, and Subcontractors. Business Associate shall not divulge, disclose, or communicate any PHI to any third party which does not comport with this Agreement without prior written approval from the Agency. Prior to the Business

Associate disclosing any PHI received from the Agency to any agent or subcontractor to enter into a written contract fully complies with the terms and conditions that are at least as restrictive as those that apply to Business Associate in this Agreement and the requirements of 45 C.F.R. § 164.504(e) and 314(a). Business Associate acknowledges and agrees that it shall be responsible to the Agency for any acts, failures or omissions of its agents or subcontractors in providing the services as if they were the Business Associate's own acts, failures or omissions, to the extent permitted by law.

4. Business Associate Responsibilities. Business Associate may make reasonable efforts to limits its only access, use or disclose the minimum necessary PHI needed to accomplish the intended functions, services, or activities on behalf of the Agency in accordance with 45 C.F.R. § 164.502(b). Business Associate shall comply with the following requirements:

   4.1. Comply with the Law. Business Associate acknowledges and agrees that it must review, understand, and comply with the applicable federal and state confidentiality and security laws, specifically, the provisions of the HIPAA rules at 45 C.F.R. § Parts 160, 162, and 164, Fla Stat 501.17, as well as any applicable amendments.

   4.2. Training. Business Associate shall familiarize its Workforce Members as defined in 45 C.F.R. § 160.103 with the requirements of this Agreement, and no less than annually, shall provide HIPAA training to any member of its Workforce that is authorized to access, use, or disclose PHI, and shall develop and implement a sanctions policy in accordance with 45 C.F.R. 164.530(e) and those required by 45 C.F.R. § 164.308 for any Workforce member, agent or subcontractor who violates this Agreement or the requirements of HIPAA.

   4.3. Disclosure of PHI. Business Associate shall not use or disclose PHI other than as permitted or required by the Agency, the Contract, this Agreement or as required by federal or state law.

   4.4. Safeguards. Business Associate will implement and maintain appropriate administrative, technical, and physical safeguards that protect the confidentiality, integrity, and privacy of PHI which Business Associate receives, creates, maintains, or transmits on behalf of the Agency.

   4.5. Use of Safeguards. Business Associate will use appropriate safeguards and comply, where applicable, with Subpart C of 45 C.F.R. Part 164 regarding Electronic PHI, to prevent the access, use, or disclosure of PHI for any purpose not in conformity with the functions, service, or activities provided on behalf of the Agency, this Agreement, or federal or state law.

   4.6. Unauthorized PHI. Business Associate shall make a good faith effort to identify any access, use, or disclosure of PHI that is not authorized under this Agreement

not permitted under the HIPAA rules and report the same to the Agency, including Breach by Business Associate or its subcontractor of Unsecured PHI, per 45 C.F.R. 164.410, and any Security Incidents.

4.6.1. Notice to the Covered Entity. Business Associate will report to the Agency within ten (10) calendar days of discovery, any access, use, or disclosure of PHI that is not authorized under this Agreement nor permitted under the HIPAA rules of which Business Associate becomes aware. Business Associate acknowledges and agrees that its failure and/or refusal to comply with the reporting requirements set forth in this paragraph shall be a material violation of this Agreement. The requisite notice shall, to the extent possible, include the full name of each Individual whose Unsecured PHI has been, or is reasonably believed by Business associate to have been, accessed, used, or disclosed during the incident, as well as Business Associate's written risk assessment which shall provide a brief description of what happened, including the date of the Breach and the date of discovery of what happened, including the date of the Breach and the date of discovery of the Breach, a description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved), as well as a description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information involved), as well as a description of what steps Business Associate is taking to investigate the Breach, to mitigate harm to Individuals, and to protect against further Breaches.

4.6.2. Notice to Individuals, Media, Secretary of Health and Human Services, and the Florida Department of Legal Affairs. Upon discovering a Breach of PHI Business Associate shall first notify the Agency regarding the pertinent details of the Breach, thereafter, upon approval of the Agency, Business Associate shall notify each Individual whose Unsecured PHI has been or is reasonably believed by Business Associate to have been accessed, acquired, used, or disclosed as a result of such breach. Additionally, if required by law, Business Associate shall notify the media, the Secretary of the U.S. Department of Health and Human Services, and the Florida Department of Legal Affairs, as follows:

4.6.2.1. Content of Notices (Generally). After approval by the Agency, Breach notification letters to Individuals shall be sent by first-class mail, to the Individual at the last known address of the Individual. If the Individual agrees to electronic notice and such agreement has not been withdrawn, notification may be made by electronic mail. The notification shall be provided in one or more mailings as information is available. If the Individual is deceased Agency may request Business Associate provide notification to Individual's next of kin or personal representative. If there is

insufficient or out-of-date contact information that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the Individual shall be provided. If there is insufficient or out-of-date contact information for 10 or more Individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of ninety (90) calendar days on the home page of Agency's website, or conspicuous notice in a major print or broadcast media in the geographic areas where the Individuals affected by the Breach likely reside. The notice shall include a toll-free number that remains active for at least ninety (90) calendar days where an Individual can learn whether his or her PHI may have been included in the Breach.

4.6.2.2. For Breaches Involving 500 or Less Individuals. If Business Associate discovers a Breach of Unsecured PHI that involves 500 or less affected Individuals, Business Associate shall first notify the Agency regarding the pertinent details of the Incident/ Breach as called for in section 4.6.1.thereafter, after the approval of the Agency, Business Associate shall provide timely notice to affected Individuals in accordance with 45 C.F.R. 164.404 and Fla. Stat 501.171, within thirty (30) calendar days. Business Associate shall maintain a log or other documentation of such breaches and, not later than sixty (60) calendar days after the end of each calendar year, provide notice to the Secretary of the U.S. Department of Health and Human Services in accordance with 45 C.F.R. 164.408(c) and shall contemporaneously submit copies of such notices to the Agency.

4.6.2.3. For Breaches Involving 500 or More Individuals. If Business Associate discovers a Breach of Unsecured PHI that involves 500 or more affected Individuals, Business Associate shall first notify the Agency regarding the pertinent details of the Incident/Breach as called for in section 4.6.1. Thereafter, after the approval of the Agency, Business Associate shall provide timely notice to affected Individuals in accordance with 45 C.F.R. 164.404 and Fla Stat. 501.171, within thirty (30) calendar days; provide timely notice to prominent media outlets in accordance with 45 C.F.R. 164.406; provide timely notice to the Florida Department of Legal Affairs by no later than thirty (30) calendar days from the date of discovering the Breach pursuant to the requirements of Fla. Stat. 501.171(3)(b); and assist the Agency in providing timely notice to the Secretary of U.S. Department of Health and Human Services by no later Than sixty (60) calendar days from the date of discovering the Breach pursuant to 45 C.F.R. 164. 408(b).

4.7. Agent or Subcontractor. In accordance with 45 C.F.R. 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, require that every agent or subcontractor of Business Associate that creates, receives, maintains, or transmits PHI on behalf of Business Associate, for the benefit of the Agency, executes a written agreement

requiring the agent or subcontractor to agree to the restrictions, conditions, and requirements that are at least as restrictive as those apply to Business Associate through this Agreement.

4.8. Individual Designated Record Set. Business Associate shall make PHI, in Designated Record Set, available to an Individual via Agency, as necessary, to satisfy the requirements of 45 C.F.R. 164.524. more specifically, within ten (10) calendar days of a request by an Individual for his or her right of access to PHI contained in a Designated Record Set Business Associate shall forward any individual requests to the Agency to fulfill such requests.

4.9. Amendments to PHI. Business Associate shall make any amendment(s) to PHI, in a Designated Record Set, as directed or agreed upon by the Agency pursuant to 45 C.F.R. 164.526, or take other measures as necessary to satisfy the Agency's obligations.

4.10. Accounting of Disclosures. Business Associate shall maintain and make available the information required to provide an accounting of disclosures to the Agency pursuant to the requirements of 45 C.F.R. 164.528. Business Associate shall document all disclosures of PHI as needed for the Agency to respond to a request for an accounting of disclosures. Within ten (10) calendar days of making a disclosure of PHI, other than disclosures excepted under 45 C.F.R. 164.528(a), Business Associate shall provide the Agency with a written report of such disclosures to the Agency for the Agency to fulfill such requests, or upon Agency request for the information.

4.10.1. At a minimum, Business Associate shall provide the following information for each disclosure: (i) the date of the disclosure; (ii) the name of the entity or person who received the PHI and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under 164.502(a)(2)(ii) or 164.512, if any. Such information must be maintained by Business Associate and its agent and subcontractor for a period of six (6) years from the date of each disclosure.

4.11. Business Associate carrying out Agency Obligations. To the extent Business Associate is to carry out one or more of the Agency's obligations under Subpart E of 45 C.F.R. 164, it shall comply with the requirements of Subpart E that apply to the Agency in the performance of such obligation(s). 45 C.F.R.§ 164.504.

4.12. HHS Compliance. Business Associate agrees to make its internal practices, books, records relating to the access, use, and disclosures of PHI received from, or created or received by Business Associate on behalf of, the Agency available to the Secretary of the U.S. Department of Health and Human Services for

purposes of determining compliance with the HIPAA rules. 45 C.F.R. § 164.504. Business Associate shall notify the Agency of the request from the U.S. Department of Health and Human Services.

4.13. Notice to Agency of PHI request. Business Associate agrees to notify the Agency within five (5) calendar days of following Business Associate's receipt of any request, subpoena, or judicial or administrative order to disclose PHI as it relates to any agreement between Business Associate and the Agency, if permitted by law. In any event, the notification shall occur before the PHI is released, in a manner that gives the Agency an opportunity to review the request and object if necessary. If the Agency decides to challenge the validity of such request, subpoena or order, Business Associate agrees to cooperate with Agency in such challenge.

4.14. Notice to Agency of Unauthorized Access. Business Associate acknowledges and agrees that any notification under this Agreement must be made the Agency's HIPAA Privacy Official regarding any incidents in which PHI is accessed, used, or disclosed for a purpose that is not authorized under this Agreement or the HIPAA rules. The Agency's HIPAA Privacy Official's contact is as follows:

HIPAA Privacy Official
Office of the General Counsel
Agency for Persons with Disabilities
4030 Esplanade Way, Suite 380
Tallahassee, Florida 32399
Telephone: (850) 922-6823
Email: HIPAA@apdcares.org

5. Covered Entity Duties

5.1. Notice of Changes to Business Associate. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.

5.2. Notice of Restriction to Business Associate. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. 164.522.

5.3. Prohibition of Improper Use or Disclosure. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity.

5.4. Contact. Covered Entity shall send all written communications to Business Associate required under this Agreement to the following contact:

Name:
Title:
Company or Agency:
Mailing Address:
Telephone:
Email:

6. Use and Disclosure of Information for Management, Administration, or Legal Responsibilities. Business Associate may not use or disclose PHI in a manner that violates the HIPAA Privacy and Security rules, if done by the Agency, or that exceeds the permitted uses set forth in this Agreement. Notwithstanding those requirements, in accordance with 45 C.F.R. 164.504(e)(4), the Agency acknowledges that Business Associate is permitted to use and disclose PHI received from the Agency for the proper management and administration of the Business Associate and to carry out the legal responsibilities of Business Associate to the extent that such disclosures are Required By Law and Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that: (1) the PHI will be held confidentiality; (2) the PHI will be used or further disclosed only as Required By Law, and (3) the person notifies Business Associate of any instance of which it is aware in which the confidentiality of the PHI has been breached. Business associate shall notify the Agency of any disclosures made under this section pursuant to section 4.13. The legal document which forms the basis of the request shall be forwarded to the Agency with this notification.

   6.1. Use PHI as Necessary per the Contract. Business Associate may use and disclose Protected Health Information as necessary in order to provide its services as described in the Contract, and as permitted by federal law and the laws of the State of Florida.

   6.2. Data Aggregation. Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. 164.504(e)(2)(i)(B).

   6.3. De-identification. Business Associate may de-identify PHI received from Covered Entity, consistent with the HIPAA Rules' standards for de-identification at 45 C.F.R. 164.514.

7. Prohibited Uses. Unless specifically stated in the "Purposes for which PHI May Be Disclosed to Business Associate" section of this Agreement, Business Associate, or any of its officers, employees, subcontractors, or agents shall not access, use, or disclose any PHI for the purposes of marketing, fundraising, or selling PHI.

8. Mitigation. Business Associate agrees to mitigate any harmful effects that arise from the unauthorized access, use, or disclosure of PHI by Business Associate in violation of the requirements of this Agreement and the HIPAA rules.

9. Indemnification. Business Associate shall indemnify and hold harmless the Agency from and against any and all losses, costs, expenses, or damages that Agency sustains as a result of, or arising out of a breach of this Agreement or the HIPAA rules by Business Associate or any of its agent or subcontractor A breach of the terms and conditions of this Agreement shall be deemed a breach of the Contract for purposes of the indemnification provisions of the Contract.

10. Term and Termination.

    10.1. Term. The term of this Agreement shall be effective upon both parties executing this Agreement and will continue until such time as the Contract has been concluded or terminated via the terms and conditions of the Contract.

    10.2. Termination Without Cause. Either party may terminate this Agreement without cause upon no less than thirty (30) calendar days' written notice to the other party unless a lesser time is mutually agreed upon, in writing, by both parties. Said notice shall be delivered by certified mail, return receipt requested, or in person with proof of delivery.

    10.3. Termination for Cause. If the Agency determines that Business Associate has violated a material term of this Agreement, the Agency may terminate this Agreement upon twenty-four (24) hours written notice to Business Associate.

    10.4. Obligations of Business Associate Upon Termination. Upon termination of this Agreement, if feasible, Business Associate shall return all PHI received from, or created, or received by Business Associate on behalf of the Agency that Business Associate still maintains in any form, including any copies or hybrid or merged databases made by Business Associate. Business Associate shall not retain any paper or electronic copies of the PHI unless approved, in writing, by the Agency. If the Agency provides Business Associate with written authorization to destroy the PHI, Business Associate must properly dispose of the PHI to ensure the PHI is no longer accessible and provide the Agency with written confirmation of such destruction of the PHI. If the return or destruction of the PHI is determined infeasible by the Agency, Business Associate shall continue to extend the protections of this Agreement to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

11. Survival. Business Associate's obligations under paragraph 10.4 shall survive the termination of this Agreement.

12. Interpretation. Each party acknowledges and agrees that it entered into this Agreement with the intention of complying with the requirements of HIPAA as well as other applicable federal and state confidentiality laws. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA rules.

13. Severability. In the event that any term or provision of this Agreement is legally determined to be unlawful or unenforceable, the remainder of this Agreement shall remain in full force and effect and such term or provision shall be stricken.

14. Regulatory References. Any reference in this Agreement to any statutory or regulatory authority means that which is currently in effect as well as any future amendments.

15. Amendments. This Agreement may not be modified or amended except in a writing duly executed by authorized representatives of both parties. The parties agree to amend this Agreement to the extent necessary to allow each party to comply with the standards and requirements of HIPAA, the HITECH Act, as well as other applicable federal and state laws relating to the security and confidentiality of PHI and/or personal information.

16. Waiver. Either party's failure to enforce any provision of this Agreement shall not, in any way, be construed as a waiver of such provision or prevent that party from enforcing it and every other provision of this Agreement.

17. Miscellaneous. If the Agency determines that Business Associate is not performing its duties under the terms and conditions of this Agreement, the Agency may, at its sole discretion, allow Business Associate a period of time to cure its deficiencies to achieve compliance.

BY SIGNING THIS AGREEMENT, EACH PARTY ACKOWLEDGES THAT IT HAS READ AND AGREED TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT AND INTEND TO BE LEGALLY BOUND BY THE SAME.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed by their authorized officials.

INSERT NAME OF PROVIDER	FLORIDA AGENCY FOR PERSONS WITH DISABILITIES
Signature	Signature
Printed Name	Printed Name
Title	Title
Date	Date