Attachment 15
Business Associate Agreement

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement"), effective _____ ("Effective Date") is made by and between **Iowa Department of Administrative Services,** (hereinafter referred to as "Plan Sponsor" or "Employer") and _____ (hereinafter referred to as "Business Associate") (collectively the "Parties"). in order to comply with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended and its implementing privacy, security and breach notification regulations ("HIPAA"), including as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act in Public Law 111-5, 42 U.S.C. § 17921-54 and its implementing regulations, each as amended (collectively, the "HITECH Act"), and any other applicable state and federal confidentiality laws, as they may be amended from time to time.

WHEREAS, the parties to this Agreement desire to establish the terms under which Business Associate may use or disclose Protected Health Information (as defined herein) such that the Plan Sponsor's plan of health care benefits ("Plan") may comply with applicable requirements of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. Parts 160-164) ("HIPAA Privacy Regulation" and/or "HIPAA Security Regulation") and the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act"), that are applicable to business associates, along with any guidance and/or regulations issued by the U.S. Department of Health and Human Services related thereto.

WHEREAS, Employer has established and maintains the Plan, which is an employee welfare benefit plan as defined by Section 3(1) of the Employee Retirement Income Security Act of 1974 ("ERISA"), and, therefore, a health plan under HIPAA;

WHEREAS, Employer has contracted with Business Associate to provide certain third party administrator services with respect to the Plan which are described and set forth in the Third Party Administrator of Medical and Dental Insurance Plan Agreement("TPA Agreement"), as may be amended from time to time;

WHEREAS, Employer is authorized to enter into this Agreement on behalf of Plan;

ARTICLE 1
DEFINITIONS

Terms used herein, but not otherwise defined, shall have meaning ascribed by Title 45, Parts 160 and 164, of the United States Code of Federal Regulations, as amended from time to time. Should any term set forth in 45 CFR Parts 160 or 164 conflict with any defined term herein, the definition found in 45 CFR Parts 160 or 164 shall prevail.

1.1 Breach. “Breach” means the acquisition, access, use, or disclosure of PHI in a manner not permitted which compromises the security or privacy of such information as defined and subject to the exceptions set forth in 45 CFR § 164.402.

1.2 Breach Notification Rule. “Breach Notification Rule” means the HIPAA Regulations pertaining to breaches of unsecured PHI as codified in 45 CFR Parts 160 and 164.

1.3 Designated Record Set. “Designated Record Set” means a group of records maintained by or for a covered entity, as defined by the HITECH Act, that is: (i) the medical records and billing records about Individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about Individuals. For purposes of this definition, the term “record” means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

1.4 Electronic PHI. “Electronic PHI” or “EPHI” means PHI that is transmitted by or maintained in electronic media as defined by the Security Rule.

1.5 Individual. “Individual” means the same as the term “individual” in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502 (g).

1.6 Law. “Law” means all applicable federal and state statutes and all relevant regulations.

1.7 Privacy Rule. “Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160 and 164, subparts A and E.

1.8 Protected Health Information (“PHI”). “Protected Health Information” or PHI has the same meaning as the term “Protected Health Information” in 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of the Plan.

1.9 Secretary. “Secretary” means the Secretary of the Department of Health and Human Services or his or her designee.

1.10 Security Incident. “Security Incident” shall have the meaning set out in the Security Rule. Generally, a “Security Incident” shall mean any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or systems operations in an electronic information system.

1.11 Security Rule. “Security Rule” means the Security Standards and Implementation Specifications at 45 CFR parts 160 and 164, subparts A and C, as they may be amended from time to time.

1.12 Unsecured PHI. “Unsecured PHI” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of either the encryption method or the destruction method, as defined in Department of Health and Human Services (“HHS”) guidance published on April 27, 2009 (74 FR 19006) and modified by guidance published on August 24, 2009 (74 FR 42740), as amended. Unsecured PHI can include information in any form or medium, including electronic, paper or oral.

ARTICLE 2
BUSINESS ASSOCIATE OBLIGATIONS

Business Associate agrees to comply with applicable federal and state confidentiality and security laws, specifically the provisions of the HITECH Act applicable to business associates (as defined by the HITECH Act), including:

2.1 Use and Disclosure of PHI. Except as otherwise permitted by this Agreement or applicable law, Business Associate shall not use, maintain, transmit or disclose PHI except as necessary to provide services to or on behalf of the Plan and except as required by Law. Business Associate may use and disclose PHI as necessary for the proper management and administration of Business Associate, or to carry out its legal responsibilities. Business Associate shall in such cases:

2.1.1 Provide information to members of its workforce using or disclosing PHI regarding the confidentiality requirements in the HITECH Act and this Agreement;

2.1.2 Obtain reasonable assurances from the person or entity to whom the PHI is disclosed that: (i) the PHI will be held confidential and further used and disclosed only as required by Law or for the purpose for which it was disclosed to the person or entity; and (ii) the person or entity will notify Business Associate of any instances of which it is aware in which confidentiality of the PHI has been breached;

2.1.3 Notify the Employer of any instances of which it is aware in which the PHI is used or disclosed for a purpose that is not otherwise provided for in this Agreement or for a purpose not expressly permitted by the HITECH Act.

2.2 Disclosure to Business Associate's Agents and Subcontractors. If Business Associate discloses PHI to agents, including a subcontractor, Business Associate shall require the agent or subcontractor to agree to the same restrictions and conditions as apply to Business Associate under this Agreement and to comply with the applicable requirements of the Privacy Rule, Security Rule, HITECH Act, Breach Notification Rule and other Law with respect to such information. Business Associate shall ensure that any agent, including a subcontractor, agrees to implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of the PHI or EPHI that it creates, receives, maintains, stores, uses or transmits on behalf of the Plan in accordance with Law. Business Associate shall be liable to the Plan for any acts, failures or omissions of the agent or subcontractor in providing the services as if they were Business Associate's own acts, failures or omissions, to the extent permitted by law. Business Associate further expressly warrants that its agents or subcontractors will be specifically advised of, and will comply in all respects with, the terms of this Agreement.

2.3 Disclosure to Plan and Employer (and their Subcontractors). Other than disclosures permitted by Section 2.1 above, Business Associate will not disclose Individuals' PHI to the

Plan, its Plan Sponsor or Employer, or any business associate or subcontractor of such parties except as set forth in Section 2.10.

2.4 Withdrawal of Authorization. If the use or disclosure of PHI in this Agreement is based upon an Individual's specific authorization for the use or disclosure of his or her PHI, and the Individual revokes such authorization, the effective date of such authorization has expired, or such authorization is found to be defective in any manner that renders it invalid, Business Associate shall, if it has notice of such revocation, expiration or invalidity, cease the use and disclosure of the Individual's PHI except to the extent it has relied on such use or disclosure, or if an exception under the HITECH Act expressly applies.

2.5 Safeguards. Business Associate agrees to maintain appropriate safeguards as required by Law, including without limitation, a written security program that contains the necessary administrative, physical and technical safeguards to ensure that PHI or EPHI is not used, maintained, transmitted or disclosed other than as provided by this Agreement or as required by Law. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of any PHI or EPHI it creates, receives, maintains, stores, uses, transmits or discloses on behalf of the Plan in accordance with Law.

Business Associate shall ensure, at a minimum, that:

2.5.1 PHI or EPHI will be maintained in locked and secured areas when PHI or EPHI is not in use;

2.5.2 Facsimile machines receiving PHI or EPHI shall not be located in a public area;

2.5.3 EPHI stored electronically shall be password protected;

2.5.4 PHI and EPHI will not be shared with outside organizations; and

2.5.5 PHI and EPHI will be used internally on a need to know basis only.

2. 6 Individual Rights

2.6.1 Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for the Plan to respond to a request by an Individual for an accounting of disclosures of PHI as required by and in accordance with 45 CFR § 164.528 as amended by the HITECH Act and its implementing regulations. Business Associate, in accordance with 45 CFR § 164.528, does not need to document disclosures of PHI that are for treatment, payment or healthcare operations or disclosures that are incidental to another permissible disclosure. If Business Associate or its agents or subcontractors uses or maintains PHI in an electronic record of health-related information created, gathered or maintained or consulted by authorized health care clinicians and staff, then Business Associate and its agents and subcontractors shall document and make available to the Plan the information required to provide an accounting of disclosures to enable the Plan to fulfill its obligations under the HITECH Act as of the date compliance is required under the HITECH Act or its implementing

regulations, including disclosures and uses relating to treatment, payment and health care operations.

2.6.2 Business Associate agrees to provide to the Plan, within thirty days of the request, in a mutually agreed upon form, information collected in accordance with 2.6.1 above to the extent required to permit the Plan to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528, as amended by the HITECH Act. The Plan shall provide to Business Associate within 30 days of the effective date of this Agreement, a written explanation of the Plan's requirements under this section (b) in sufficient detail to enable the Plan to comply with such requirements. The Plan agrees to respond promptly to requests from Business Associate for clarification of such requirements, and Business Associate may rely on such responses. The Parties agree to work together in good faith to resolve any disagreement over the requirements of 45 CFR § 164.528, as amended by the HITECH Act. The Plan will be responsible for the reasonable costs incurred by Business Associate to respond to a request for an accounting of disclosures. The Plan, rather than Business Associate, will directly handle all requests for accounting from an Individual. Business Associate shall promptly forward all requests for accounting it receives from Individuals to the Plan.

2.6.3 Business Associate shall, at the request of the Plan, provide PHI maintained in a Designated Record Set to the Plan or, as directed by the Plan, to an Individual in order to meet the requirements of an Individual's right of access and requests for access to his or her PHI. An Individual's right of access to PHI includes the right to access EPHI contained in an electronic health record. The Plan will be responsible for the reasonable costs incurred by Business Associate to respond to a request for access. The provision of access to the Individual's PHI or EPHI and any denials of access to PHI or EPHI shall be the sole responsibility of the Plan. If Business Associate or its agents or subcontractors maintains or uses PHI, then promptly after receipt of a request from the Plan, Business Associate shall make a copy of such PHI available to the Plan in an electronic format in order to enable the Plan to fulfill its obligations under the HITECH Act and the Privacy Rule.

2.7 De-identified Information. Business Associate may use and disclose de-identified health information if (i) the use is disclosed to the Plan and permitted by law and (ii) the de-identification is in compliance with 45 CFR §164.502(d) and (iii) the de-identified health information meets the standard and implementation specifications for de-identification under 45 CFR §164.514(a) and (b).

2.8 Minimum Necessary. Business Associate shall attempt to ensure that all uses and disclosures of PHI are subject to the principle of "minimum necessary use and disclosure," i.e., that only PHI that is the minimum necessary to accomplish the intended purpose of the use, disclosure or request is used or disclosed.

2.9 Notice of Privacy Practices. Business Associate shall abide by the limitations of the Plan's notice of privacy practices ("Notice of Privacy Practices") of which it has knowledge. Any use or disclosure permitted by this Agreement may be amended by changes to the Plan's Notice of Privacy Practices; provided, however, that the amended Notice of Privacy Practices shall not affect permitted uses and disclosures on which Business Associate relied prior to receiving notice of such amended Notice of Privacy Practices.

2.10 Disclosures of Protected Health Information. The following provisions apply to disclosures of Protected Health Information to the Plan, Employer and other business associates of the Plan.

2.10.1 Disclosure to Plan. Unless otherwise provided by this Section 2.10, all communications of Protected Health Information by Business Associate shall be directed to the Plan.

2.10.2 Disclosure to Employer. Business Associate may provide Summary Health Information regarding the Individuals in the Plan to Employer upon Employer's written request for the purpose either (a) to obtain premium bids for providing health insurance coverage for the Plan, or (b) to modify, amend or terminate the Plan. Business Associate may provide information to Employer on whether an individual is participating in the Plan or is enrolled in or has disenrolled from any insurance coverage offered by the Plan.

2.10.3 Disclosure to Other Business Associates and Subcontractors. Business Associate may disclose Individuals' Protected Health Information to other entities or business associates of the Plan if the Plan authorizes Business Associate in writing to disclose Individuals' Protected Health Information to such entity or business associate. The Plan shall be solely responsible for ensuring that any contractual relationships with these entities or business associates and subcontractors comply with the requirements of 45 Code of Federal Regulations § 164.504(e) and § 164.504(f).

2.11 Security Incident / Unauthorized Disclosure of PHI.

2.11.1 Business Associate shall report to the Plan any instances, including Security Incidents, of which it is aware in which PHI or EPHI is used or disclosed for a purpose that is not otherwise provided for in this Agreement. In the event that Business Associate knows of: (i) any suspected Breach of any individual PHI or EPHI; (ii) a Security Incident (i.e. PHI was inappropriately used, disclosed, released or obtained) or (iii) a Breach of Unsecured PHI, Business Associate shall notify the Plan in writing within five (5) calendar days of such Breach. Notification shall include detailed information about the Breach, including, but not limited to, the nature and circumstances of such Breach, the means by which PHI or EPHI was or may have been breached (e.g. stolen laptop; breach of security protocols; unauthorized access to computer systems, etc.), the names and contact information of all individuals affected or reasonably believed by the Business Associate to be affected, and such other information as the Plan may reasonably request. Any delay in notification must include evidence demonstrating the necessity of the delay. The notice shall also set forth the remedial action taken or proposed to be taken with respect to such prohibited use or disclosure. Business Associate and the Plan agree to act together in good faith to take reasonable steps to

investigate and mitigate any harm caused by such unauthorized use or successful Security Incident. The Party responsible for the breach shall bear the cost of any required notifications and corrective actions (e.g. credit monitoring services). The Business Associate will provide the Plan with any reasonable information known by Business Associate that the Plan needs for the required notifications under the Breach Notification Rule. The Plan shall have responsibility for determining that an incident is a Breach, including the requirement to perform a risk assessment. However, the Business Associate is expected to perform a risk assessment and provide such assessment to the Plan. Further, Business Associate shall provide and pay for required notifications to Individuals, HHS and/or the media, as requested by the Plan.

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

2.12 Prohibited Actions. With respect to PHI and EPHI, Business Associate agrees not to:

2.12.1 Directly or indirectly receive remuneration in exchange for any PHI as prohibited by, and subject to the exceptions under the HITECH Act, Privacy Rule, and state law as of their respective compliance dates.

2.12.2 Make or cause to be made any communication about a product or service that encourages recipients of the communication to purchase or use the product or service as prohibited by, and subject to the exceptions under the HITECH Act and the Privacy Rule, as of their respective compliance dates. Business Associate agrees to comply with applicable federal and state Law regarding marketing communications involving the use of disclosure of PHI; and

2.12.3 Make or cause to be made any written fundraising communications that is a Health Care Operation without provision, in a clear and conspicuous manner, of an opportunity for the recipient to elect not to receive further fundraising communications in accordance with the HITECH Act and the Privacy Rule as of their respective compliance dates. Business Associate further agrees to comply with all applicable Law regarding the use of PHI for fundraising communications.

ARTICLE 3
THE PLAN'S OBLIGATIONS

3.1 If applicable to the Plan under the Law, the Plan shall:

3.1.1 Provide Business Associate a copy of its Notice of Privacy Practices produced by the Plan in accordance with 45 CFR 164.520 as well as any changes to such notice;

3.1.2 Provide Business Associate with any changes in, or revocation of, authorizations by Individuals relating to the use and/or disclosure of PHI, if such changes affect Business Associate's permitted or required uses and/or disclosures;

3.1.3 Notify Business Associate of any restriction to the use and/or disclosure of PHI to which the Plan has agreed in accordance with 45 CFR 164.522;

3.1.4 Notify Business Associate of any amendment to PHI to which the Plan has agreed that affects a Designated Record Set maintained by Business Associate; and

3.1.5 If Business Associate maintains a Designated Record Set, provide Business Associate with a copy of its policies and procedures related to an Individual's right to: access PHI; request an amendment to PHI; request confidential communications of PHI; or request an accounting of disclosures of PHI.

ARTICLE 4
MUTUAL OBLIGATIONS

4.1 Confidential Information. Both Parties acknowledge that in the course of performing under this Agreement, each Party may learn or receive confidential, trade secret or other proprietary information ("Confidential Business Information") concerning the other Party, or third parties to whom the other Party has an obligation of confidentiality. Each Party shall take all necessary steps to provide the maximum protection to the other Party's Confidential Business Information and records. Each Party agrees to take at least such precautions to protect the other Party's Confidential Business Information as it takes to protect its own Confidential Business Information, but shall in no instance less than a reasonable degree of care. Such information shall not be disclosed to third parties without the express written consent of the Party to whom the information belongs. The Parties shall not utilize any Confidential Business Information belonging to the other Party other than as expressly permitted by this Agreement or otherwise in writing or as required by Law. Each Party shall retain sole ownership of its own Confidential Business Information.

4.2 Electronic Transactions and Code Sets. Both Parties understand and agree that they are required to comply with the HIPAA Standards for Electronic Transactions, 45 CFR Parts 160 and 162 (HIPAA Electronic Transaction Law) as amended from time to time. The HIPAA Electronic Transaction Law requires Business Associate to conduct certain transactions as "standard transactions" using defined medical data code sets. Business Associate agrees that it will require its subcontractors, vendors, and independent contractors to comply with HIPAA Electronic Transaction Law as applicable. Business Associate agrees that it will not:

4.2.1 Change the definition, data condition, or use of a data element or segment in a standard;

4.2.2 Add any data elements or segments to the maximum defined data set;

4.2.3 Use any code or data elements that are either marked "not used" or not included in the standard's implementation specification(s); or

4.2.4 Change the meaning or intent of the standard's implementation specification(s).

.

ARTICLE 5
TERM AND TERMINATION

5.1 This Agreement will continue in full force and effect for as long as the TPA Agreement remains in full force and effect. This Agreement will terminate upon the cancellation, termination, expiration or other conclusion of the TPA Agreement.

5.2 Termination for Breach. Either Party may terminate this Agreement in the event of material breach by the other Party, upon thirty (30) days' prior written notice, unless the breach is cured during the notice period.

5.3 Effect of Termination. Upon termination of this Agreement for any reason, Business Associate agrees to return or destroy all PHI maintained by Business Associate in any form. If Business Associate determines that the return or destruction of PHI is not feasible, Business Associate shall inform the Plan in writing of the reason thereof, and shall agree to extend the protections of this Agreement to such PHI and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the PHI not feasible for so long as Business Associate retains the PHI.

ARTICLE 6
MISCELLANEOUS

6.1 Rights of Proprietary Information. The Plan retains any and all rights to the proprietary information, confidential information, and PHI it releases to Business Associate.

6.2 Survival. The respective rights and obligations of Business Associate with regard to the return of records to the Plan shall survive the termination of the Agreement.

6.3 Notices. Any notices pertaining to this Agreement shall be given in writing and shall be deemed duly given when personally delivered to a Party or a Party's authorized representative at the respective address indicated herein or sent by means of a reputable overnight carrier or certified mail, return receipt requested, postage prepaid. A notice sent by certified mail shall be deemed given on the date of receipt or refusal of receipt.

6.4 Amendments. This Agreement may not be changed or modified in any manner except by an instrument in writing signed by a duly authorized officer of each of the Parties hereto. Amendments as determined by the Plan to be necessary to effect compliance with legislative, regulatory, or other legal authority do not require the consent of Business Associate and shall be effective immediately upon Business Associate's receipt from the Plan of notice of amendment.

6.5 Choice of Law. This Agreement and the rights and the obligations of the Parties hereunder shall be governed by and construed under the laws of the State of Iowa, without regard to applicable conflict of laws principles.

6.6 Assignment of Rights and Delegation of Duties. This Agreement is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns.

However, neither Party may assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Notwithstanding any provisions to the contrary, however, the Plan retains the right to assign or delegate any of its rights or obligations hereunder to any of its wholly owned subsidiaries, affiliates, or successor companies. Assignments made in violation of this provision are null and void.

6.7 Nature of Agreement. Nothing in this Agreement shall be construed to create (i) a partnership, joint venture or other joint business relationship between the Parties or any of their affiliates, or (ii) a relationship of employer and employee between the Parties.

6.8 No Waiver. Failure or delay on the part of either Party to exercise any right, power, privilege, or remedy hereunder shall not constitute a waiver thereof. No provision of this Agreement may be waived by either Party except by a writing signed by an authorized officer of the Party making the waiver.

6.9 Severability. The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

6.10 No Third Party Beneficiaries. Nothing in this Agreement shall be considered or construed as conferring any right or benefit on a person not Party to this Agreement nor imposing any obligations on either Party hereto to persons not a Party to this Agreement.

6.11 Headings. The descriptive headings of the articles, sections, subsections, exhibits, and schedules of this Agreement are inserted for convenience only, do not constitute a part of this Agreement and shall not affect in any way the meaning or interpretation of this Agreement. All pronouns and any variations thereof are deemed to refer to the masculine, feminine, neuter, singular, or plural as the identity of the person or persons may require.

6.12 Entire Agreement. This Agreement, together with all the exhibits, riders and amendments, if applicable, which are fully completed and signed by authorized persons on behalf of both Parties from time to time while this Agreement is in effect, constitutes the entire Agreement between the Parties hereto with respect to the subject matter hereof and supersedes all previous or contemporaneous written or oral understandings, agreements, negotiations, commitments, and any other writing and communication by or between the Parties with respect to the subject matter hereof. In the event of any inconsistencies between any provisions of this Agreement in any provisions of the exhibits or riders, the provisions of this Agreement shall control.

6.13 Regulatory References. A citation in this Agreement to the Code of Federal Regulations means the cited section as that section may be amended from time to time.

6.14 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Plan to comply with the HITECH Act. The provisions of this Agreement shall prevail over the provisions of any other agreement that exists between the Parties that may conflict with, or appear inconsistent with, any provision of this Agreement or the HITECH Act.

Date: _____

Business Associate:

By: _____
Name:
Title:

Date: _____

IOWA DEPARTMENT OF ADMINISTRATIVE SERVICES

By: _____
Name:
Title: