BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("BAA") is part of each written agreement between Emtelligent and Customer that expressly incorporates this BAA (the "Agreement"). This BAA applies only to the processing of Protected Health Information subject to HIPAA (as defined below). To the extent of any conflict with our Data Protection Agreement, this BAA shall control.

RECITALS

A. Covered Entity is a health care provider subject to the Health Insurance Portability and Accountability Act of 1996, the HITECH Act, and regulations promulgated thereunder ("HIPAA").

B. Business Associate, through the provision of services on behalf of the Covered Entity pursuant to one or more services agreement entered into between the parties (the "Services Agreement"), is a "business associate" of the Covered Entity as that term is defined in 45 C.F.R. § 160.103, and is subject to the Security Rule and certain provisions of the Privacy Rule.

C. Covered Entity is required by HIPAA to obtain satisfactory assurances that Business Associate will appropriately safeguard all Protected Health Information and Electronic Protected Health Information disclosed by, or created or received by Business Associate on behalf of, Covered Entity.

NOW, THEREFORE, in consideration of entering into the Services Agreement and the mutual promises and agreements below and in order to comply with all legal requirements, the parties agree as follows:

I. DEFINITIONS

1.1 "Agreement" has the meaning set forth in the preamble.

1.2 "Breach**"** has the same meaning as the term "Breach" in Section 13400(1) of the HITECH Act (i.e. 42 USCA 17921) and 45 C.F.R. § 164.402.

1.3 "Business Associate" has the meaning set forth in the preamble, and for purposes of this BAA, refers to Emtelligent.

1.4 "Covered Entity" has the meaning set forth in the preamble, and for purposes of this BAA, refers to Customer.

1.5 "Data Aggregation" means the combining of PHI created or received under this Agreement with the PHI Business Associate receives or creates in its arrangement with another covered entity under the Privacy Rule to permit data analysis that relate to the Health Care Operations of the covered entities.

1.6 "Designated Record Set" means a group of records maintained by or for the Covered Entity that is: (i) the medical records and billing records about Individuals; (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. As used herein the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the Covered Entity.

1.7 "Effective Date" has the meaning set forth in the preamble.

1.8 "Electronic PHI" means information that comes within paragraphs 1(i) or 1(ii) of the definition of "protected health information," as defined in 45 C.F.R. § 160.103, limited to the information created, received, maintained or transmitted by Business Associate on behalf of Covered Entity.

1.9 "HIPAA" has the meaning set forth in the Recitals.

1.10 "HITECH Act" means Title XIII and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law No. 111-5 and all regulations promulgated thereunder.

1.11 "Individual" means the person who is the subject of the PHI and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.12 "PHI" means Protected Health Information that is provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity.

1.13 "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.

1.14 "Protected Health Information" means any information, whether transmitted or maintained in electronic, written, oral, or any other form or medium, that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual; and (i) identifies the Individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

1.15 "Required by Law" has the same meaning as the term "'required by law" in 45 C.F.R. § 164.103.

1.16 "Secretary" means the Secretary of the U.S. Department of Health and Human Services or his or her designee.

1.17 "Security Incident" has the same meaning as the term "security incident" in 45 C.F.R. § 164.304." It does not include inconsequential incidents that occur on a frequent basis such as scans or "pings" that are not allowed past Business Associate's firewall.

1.18 "Security Rule" means the Security Standards and Implementation Specifications at 45 C.F.R. part 160 and part 164, subpart C.

1.19 "Services Agreement" has the meaning set forth in the Recitals.

1.20 **"Subcontractor"** has the meaning set forth in 45 C.F.R. § 160.103.

1.21 "Unsecured Protected Health Information" or "Unsecured PHI" means PHI that is not secured through the use of a technology or methodology that the Secretary specifies in guidance renders PHI unusable, unreadable, or indecipherable to unauthorized Individuals, such as the guidance set forth in 74 Fed. Reg. 19006 (April 27, 2009) and updated in 74 Fed. Reg. 42740 (August 24, 2009).

1.22 Remaining Terms. Capitalized terms used, but not otherwise defined, in this Agreement have the meaning ascribed to them in HIPAA, the Privacy Rule, the Security Rule or the HITECH Act.

II. PERMITTED USES AND DISCLOSURES OF PHI

2.1 **Services Agreement Uses and Disclosures**. Business Associate may use or disclose PHI for purposes of performing its obligations and functions under the Services Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

2.2 **Other Permitted Uses**. If necessary, Business Associate may use PHI: (i) for the proper management and administration of the Business Associate; (ii) to carry out the legal responsibilities of the Business Associate; and (iii) for the provision of Data Aggregation services relating to the Health Care Operations of Covered Entity. Business Associate may de-identify PHI and use such de-identified data for its own internal purposes.

2.3 **Other Permitted Disclosures**. If necessary, Business Associate may disclose PHI for the purposes described in Section 2.2 above if: (i) the disclosure is Required by Law; or (ii) Business Associate obtains reasonable written assurance from the person or entity to whom it discloses the PHI that the PHI will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person or entity, and the person or entity notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

III. OBLIGATIONS OF BUSINESS ASSOCIATE

3.1 **Compliance with Privacy Rule.** Business Associate shall comply with all applicable provisions of the Privacy Rule in carrying out its obligations under the Services Agreement and this Agreement. Further, to the extent Business Associate is to carry out any of Covered Entity's obligations under subpart E of 45 CFR 164, Business Associate agrees to comply with the requirements of such subpart that apply to Covered Entity in the performance of such obligations.

3.2 **Prohibition on Unauthorized Use or Disclosure**. Business Associate shall not use or disclose PHI except as permitted by this Agreement or as Required by Law.

3.3 Minimum Necessary.

(a) Business Associate shall limit its use and disclosure of PHI under this Agreement to the minimum necessary to accomplish the Business Associate's intended purpose. Business Associate may in good faith determine what constitutes the minimum necessary to accomplish the intended purpose of any disclosure of PHI.

(b) Paragraph (a) above does not apply to: (1) disclosures to or requests by a health care provider for treatment; (2) uses or disclosures made to the Individual; (3) disclosures made pursuant to an authorization as set forth in 45 C.F.R. § 164.508; (4) disclosures made to the Secretary under 45 C.F.R. part 160, subpart C; (5) uses or disclosures that are Required by Law as described in 45 C.F.R. § 164.512(a); and (6) uses or disclosures that are required for compliance with applicable requirements of the Privacy Rule.

3.4 Safeguarding PHI; Security Regulations. Business Associate shall use appropriate administrative, physical, and technical safeguards and comply with the Security Rule with respect to Electronic PHI to prevent the use or disclosure of PHI other than as provided for by this BAA.

3.5 Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Security Incident or a use or disclosure of PHI by Business Associate in violation of this BAA.

3.6 Reporting. In the event that Business Associate becomes aware of a use or disclosure of PHI by Business Associate that is not permitted under this Agreement, Business Associate shall report such use or disclosure to the Covered Entity without undue delay. Business Associate agrees to report to Covered Entity in writing any Security Incident of which it becomes aware, except that, for purposes of this reporting requirement the term "Security Incident" does not include inconsequential incidents that occur on a frequent basis such as scans or "pings" that are not allowed past Business Associate's firewall. Notwithstanding this Section 3.6, the Business Associate's reporting obligations regarding any Breach are set forth in Article IV.

3.7 Subcontractors. Business Associate shall ensure that all Subcontractors or agents of Business Associate that create, receive, maintain or transmit PHI on behalf of the Business Associate agree in writing to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Business Associate shall ensure that all agents, including Subcontractors, to whom it provides Electronic PHI, agree in writing to implement reasonable and appropriate safeguards to protect such Electronic PHI.

3.8 Access.

(a) Within twenty (20) days of a request from Covered Entity, Business Associate shall furnish the PHI contained in a Designated Record Set that will enable the

Covered Entity to respond to an Individual's request for inspection or copies of PHI about the Individual pursuant to 45 CFR § 164.524.

(b) In the event an Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to the Covered Entity immediately and take no direct immediate action on any such request. If the Covered Entity determines that an Individual is to be granted access to PHI, then Business Associate shall cooperate with the Covered Entity to provide to any Individual, at the Covered Entity's direction, any PHI requested by such Individual.

3.9 Amendment.

(a) If the Covered Entity requests that Business Associate amend any Individual's PHI or a record regarding an Individual contained in a Designated Record Set, then Business Associate shall provide the relevant PHI to the Covered Entity for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526.

(b) In the event an Individual requests directly to Business Associate that PHI be amended, Business Associate shall forward such request to the Covered Entity within twenty (20) days of Business Associate's receipt of such request and shall take no direct immediate action on the request.

3.10 Records Availability. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining Covered Entity's compliance with the Privacy Rule.

3.11 Accounting of Disclosures.

(a) If the Covered Entity requests that Business Associate furnish an accounting of disclosures of PHI made by Business Associate regarding an Individual during the six (6) years prior to the date on which the accounting was requested, then Business Associate shall, within twenty (20) days of such request, make available to the Covered Entity such information as is in Business Associate's possession and is required for the Covered Entity to make the accounting required by 45 C.F.R. §164.528.

(b) In the event an Individual requests an accounting of disclosures directly from Business Associate, Business Associate shall within ten (10) days forward such request to the Covered Entity and shall take no direct action on the request.

IV. BREACH NOTIFICATION.

4.1 Risk Assessment by Business Associate. If Business Associate becomes aware of a potential Breach, Business Associate shall complete a risk assessment of the potential Breach to determine whether the potential Breach is a Breach. Such risk assessment shall include at least all the factors identified in the Security Rule.

4.2 Notification to Client. If, after completing such risk assessment, Business Associate concludes that there was a Breach, Business Associate shall notify Client of the Breach as soon as reasonably possible, and in all cases within ten (10) business days of Business Associate confirming that a Breach occurred. The notification to Client shall include, if known, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed during such Breach. The notification shall also include: (a) a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known; (b) a description of the types of Unsecured PHI that were involved in the Breach; (c) recommended steps that Individuals should take to protect themselves from potential harm resulting from the Breach; and (d) a brief description of what the Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches. Business Associate shall maintain evidence to demonstrate that any required risk assessment was completed and notification to Client under this paragraph was made unless the Business Associate determines that a delayed notice (as described in Section 4.3) applies.

4.3 Delayed Notification. Notwithstanding section 4.2 above, if the notification required under section 4.2 would impede a criminal investigation or cause damage to national security, then business associate may delay the notification for any period of time set forth in the written statement of the law enforcement official. Business Associate shall be obligated to maintain evidence to demonstrate the reason for the delayed notification and that the required notification under this paragraph was made.

V. TERM AND TERMINATION

5.1 Term. This Agreement is effective upon the effective date of the Services Agreement, and except for the rights and obligations set forth in this Agreement specifically surviving termination, shall terminate automatically on the date the Services Agreement terminates.

5.2 Termination for Cause. Notwithstanding any provision in this Agreement, if Covered Entity reasonably determines that Business Associate has breached any provision of this Agreement or otherwise violated HIPAA, the Privacy Rule, the Security Rule or the HITECH Act, Covered Entity shall provide written notice to Business Associate with an opportunity for Business Associate to cure the breach or end the violation within thirty (30) business days of such written notice, unless cure is not possible. If Business Associate fails to cure the breach or end the violation within the specified time period or cure is not possible, this Agreement and the Service Agreement shall automatically and immediately terminate, unless termination is infeasible.

5.3 Obligations Upon Termination.

(a) Except as provided in paragraph (b) of this Section 5.3, upon termination, cancellation, expiration or other conclusion of this Agreement, for any reason, Business Associate shall return or, destroy PHI in whatever form or medium and retain no copies of such

PHI. Business Associate shall complete such return or destruction as soon as reasonably possible.

(b) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VI. GENERAL PROVISIONS

6.1 Effect. The terms and provisions of this Agreement supersede any other conflicting or inconsistent terms and provisions in any agreements between the parties, including all exhibits or other attachments thereto and all documents incorporated therein by reference.

6.2 Amendment. Business Associate and the Covered Entity agree to amend this Agreement to the extent necessary to allow either party to comply with HIPAA, the Privacy Rule, the Security Rule, or the HITECH Act. All such amendments shall be made in a writing signed by both parties.

6.3 No Third Party Beneficiaries. This Agreement is intended for the benefit of Business Associate and Covered Entity only. Nothing express or implied is intended to confer or create, nor be interpreted to confer or create, any rights, remedies, obligations or liabilities to or for any third-party beneficiary, including without limitation Individuals who are the subject of PHI.

6.4 Counterparts; Facsimile Signature. This Agreement may be executed by facsimile and/or in counterparts, each of which shall be an original and all of which together shall constitute one and the same binding instrument.

6.5 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with HIPAA, the Privacy Rule, the Security Rule, and the HITECH Act.