HIPAA Compliance

Business Associate Agreement

These Standard HIPAA Business Associate Agreement Terms and Conditions ("HIPAA Addendum") shall be incorporated into the Service Agreement for Customers that are Covered Entities (as defined below) and that provide Protected Health Information ("PHI")(as defined below) to KleerMessage in connection with the services they have purchased. These terms supplement and are made part of the purchase agreement between KleerMessage and Customers ("Underlying Agreement") in order to comply with the federal Standards for Privacy of Individually Identifiable Health Information, located at 45 C.F.R. Part 160 and Part 164, Subparts A through E ("Privacy Rule") and the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH Act").

WHEREAS, in order to ensure that Covered Entity and Business Associate remain in compliance with the HIPAA Rules and other applicable federal and state laws and regulations regarding the disclosure of PHI to Business Associate, the parties have agreed to enter into this Agreement.

NOW THEREFORE, Covered Entity and Business Associate agree as follows:

1. **DEFINITIONS**

   Capitalized terms used in this Agreement and not otherwise defined herein shall have that meaning given to them in the HIPAA Rules."Breach" when capitalized, shall have the meaning set forth in 45 CFR § 164.402 (including all of its subsections); with respect to all other uses of the word "breach" in this Agreement, the word shall have its ordinary contract meaning."Electronic Protected Health Information" or "EPHI" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, limited to information that Business Associate creates, accesses or receives from or on behalf of Covered Entity."Individually Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and; is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 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 provision of health care to an individual; and

- that identifies the individual; or
- with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Protected Health Information" or **"PHI"** shall have the meaning set forth in the Privacy Rule, limited to information that Business Associate creates, accesses or receives from or on behalf of Covered Entity. PHI includes EPHI.

"Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 CFR parts 160 and 164, Subparts A, D and E, as currently in effect.

"Security Incident" shall have the same meaning as the term "security incident" at 45 CFR 164.304.

"Security Rule" means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160 and 164, Subpart C, as currently in effect.

"Unsecured Protected Health Information" or **"Unsecured PHI"** shall have the same meaning as the term "unsecured protected health information" in 45 CFR § 164.402, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATES

i. **Business Associate Status** Business Associate acknowledges and agrees that it is a "Business Associate" as defined by the HIPAA Rules, and as such, Business Associate shall, in addition to complying with the other terms and conditions of the Terms of Service Agreement, comply with the HIPAA-required provisions set forth in this Agreement. In the event of a conflict between the terms of this Agreement and the Terms of Service Agreement with respect to the use or disclosure of PHI, the terms of this Agreement will govern. In all other circumstances, the terms of the Terms of Service Agreement will govern.

ii. **Performance of Services** Business Associate may use PHI only to perform the services and its other obligations pursuant to the Terms of Service Agreement or as Required by Law. Business Associate may disclose such PHI only within its organization and only to those of its employees who need to know such information in order to perform its obligations under the Terms of Service Agreement and, in such case, only the minimum amount of such PHI as is necessary for such performance. Business Associate shall not access, use or disclose PHI in any manner that would violate the HIPAA Rules if such access, use or disclosure was done by Business Associate or Covered Entity,

iii. **Privacy Rule Obligations** Business Associate shall comply with the Privacy Rule as it directly applies to business associates: To the extent Business Associate carries out one or more of Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with the requirements of HIPAA that apply to Business Associate or Covered Entity in the performance of such obligation(s).

iv. **Safeguards for Protection of PHI** Business Associate agrees that it will (a) protect and safeguard from any disclosure (whether oral, written or otherwise) all PHI with which it may come into contact with in accordance with the HIPAA Rules and more stringent state laws and regulations governing the handling of such information; and (b) use appropriate safeguards to prevent use or disclosure of PHI other than as permitted by the Terms of Service Agreement or this Agreement or as Required by Law.

v. **Mitigation** 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.

vi. **Notification** Without unreasonable delay, and in no case later than ten (10) days after Business Associate knew or should have known of the impermissible use or disclosure, Business Associate shall notify Covered Entity, in writing, of any use or disclosure of PHI outside the purpose of this Agreement or the Terms of Service Agreement. Without unreasonable delay, Business Associate r shall report to Covered Entity in writing of any Security Incident of which it becomes aware. In addition, upon Covered Entity's request, Business Associate shall provide a report of any and all impermissible uses, disclosures, and/or Security Incidents.

vii. **Disclosure to Subcontractors** Business Associate agrees to ensure that any subcontractor that creates receives, maintains or transmits EPHI originating

from the Covered Entity on behalf of the Business Associate, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

viii. **Right of Access** Business Associate agrees to provide access, at the request of Covered Entity, to PHI contained in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in in a time and manner that allows Covered Entity to meet the requirements under 45 CFR § 164.524.

ix. **Right to Amendment** 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 CFR § 164.526 at the request of Covered Entity, in a time and manner that allows a Covered Entity to meet the requirements of 45 CFR 164.526. Business Associate shall notify Covered Entity immediately in writing upon receiving a request from an Individual to review, copy or amend his or her medical record information.

x. **Patient Right to Request Accounting** Upon Covered Entity's request, Business Associate shall document and make available to Covered Entity information relating to such Individual as is necessary for Covered Entity to respond to a request for an accounting of disclosures in accordance with §164.528 of the Privacy Rule.

xi. **Access to Books and Records** Until the expiration of four years after the furnishing of services pursuant to the Terms of Service Agreement, Business Associate agrees to make 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, for purposes of the Secretary determining compliance with the Privacy Rule.

xii. **Breach Notification** If Business Associate has knowledge or a reasonable belief that a Breach of Unsecured PHI has occurred or may have occurred, Business Associate shall notify Covered Entity in accordance with the requirements of 45 CFR § 164.410. For avoidance of doubt, Business Associate shall notify Covered Entity if it has knowledge of a potential Breach so that Covered Entity may determine and confirm whether a Breach has occurred. Such notification shall include, to the extent possible, the identification of each Individual whose PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed during the Breach, along with any other information that Covered Entity will be required to include in its notification to the Individual, the media and/or the Secretary, as applicable, including, without

limitation, a description of the Breach, the date of the Breach and its discovery, the types of Unsecured PHI involved and a description of the Business Associate's investigation, mitigation and prevention efforts.

xiii. **Security Incidents** Business Associate shall track and monitor all Security Incidents. Business Associate shall report a successful Security Incident in accordance with Section xii above and shall report unsuccessful Security Incidents upon request by Covered Entity.

xiv. **Minimum Necessary** When using, disclosing or requesting PHI, Business Associate agrees to use, disclose or request the minimal amount of information necessary for the stated purpose, unless an exception to the minimum necessary rule applies, as set forth in 45 CFR §164.502(b)(2).

3. **PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE** Business Associate shall be permitted to use and disclose PHI as follows:Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in this Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted under 45 CFR § 164.504(e)(2)(i)(B). Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).
4. **PERMITTED OBLIGATIONS OF COVERED ENTITY**Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect

Business Associate's use or disclosure of PHI.Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.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 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.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.

5. **TERMINATION**

- **Term** Business Associate acknowledges and agrees that it is a "Business Associate" as defined by the HIPAA Rules, and as such, Business Associate shall, in addition to complying with the other terms and conditions of the Terms of Service Agreement, comply with the HIPAA-required provisions set forth in this Agreement. In the event of a conflict between the terms of this Agreement and the Terms of Service Agreement with respect to the use or disclosure of PHI, the terms of this Agreement will govern. In all other circumstances, the terms of the Terms of Service Agreement will govern.
- **Effect of Termination; Return of Covered Entity's PHI** Upon termination of the Terms of Service Agreement for any reason, Business Associate will return or destroy all PHI within thirty (30) days of the date of termination. Business Associate will not retain any records or copies of any such records. To the extent the return or destruction of such PHI is not feasible, Business Associate will remain bound by the provisions of this Agreement even after termination of the Terms of Service Agreement, until such time as all PHI has been returned or is destroyed.
- **Survival** The obligations of Business Associate under this Section 5 shall survive the termination of this Agreement and remain in force as long as Business Associate stores or maintains PHI in any form or format.

6. **MISCELLANEOUS**

- **Amendments** This Agreement may not be modified in any respect other than by a written instrument signed by both parties.
- **Severability** In the event any part or parts of this Agreement are held to be unenforceable, the remainder of this Agreement will continue in effect.

- **Governing Law** To the extent not preempted by Federal law, this Agreement shall be governed and construed in accordance with the state laws governing the Terms of Service Agreement, without regard to conflicts of law provisions.
- **Interpretation** Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.
- **No Third Party Beneficiaries** Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assigns of the parties, any rights, remedies, obligations, or liabilities whatsoever.