ero HEALTH
A Med Tech Solutions Partner

BUSINESS ASSOCIATE PROVISIONS

Section 1
Definitions

Capitalized terms used, but not otherwise defined, in this Agreement shall have the meanings given those terms in the HIPAA Privacy and Security Rules and HITECH.

1.1 ***Breach:*** "Breach" shall mean an acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, which compromises the security or privacy of the PHI. For the purposes of this definition, a breach is presumed to be a breach unless the Covered Entity (CE) or Business Associate (BA), as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a four-factor risk assessment as amended in the Final HIPAA Omnibus Rule in §164.402(2).

Breach excludes:

a. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA), if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
b. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
c. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

1.2 ***Business Associate:*** shall mean Ero Health

1.3 ***Covered Entity:*** "Covered Entity" shall mean Client

1.4 ***Electronic Health Record:*** "Electronic Health Record" shall mean an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

1.5 ***Electronic Protected*** **Health Information:** "Electronic Protected Health Information" shall mean Protected Health Information that is created, received, transmitted or maintained in electronic format or by electronic media.

1.6 ***Individual:*** "Individual" shall have the same meaning as the term "Individual" in 45 C.F.R. §164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502(g).

1.7 ***Privacy Rule:*** "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. parts §160 and §164, Subparts A and E.

1.8 ***Protected Health Information:*** "Protected Health Information" shall have the same meaning as the term "Protected Health Information" 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 ***Security Incident:*** "Security Incident" shall have the same meaning as the term "Security Incident" in 45 C.F.R. §164.304. Notwithstanding the foregoing, the Parties acknowledge and agree that Business Associate need not report all attempted but unsuccessful Security Incidents to Covered Entity, and that this Agreement constitutes notice to Covered Entity that such unsuccessful Security Incidents occur periodically. Unsuccessful Security Incidents include, but are not limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as such incidents do not result in actual unauthorized access, use, or disclosure of PHI.

1.10 ***Security Rule:*** "Security Rule" shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. parts §160 and §164, Subparts A and C

1.11 ***Unsecured Protected Health Information or Unsecured PHI:*** "Unsecured PHI" shall mean protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of the HITECH Act.

1.12 ***Secretary:*** "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

Section 2
Obligations and Activities of Business Associate

Business Associate agrees to the following:

2.1 ***Not Use or Disclose PHI Unless Permitted or Required.*** Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by this Agreement, the underlying or as Required by Law, for the proper management and administration of the BA, or as otherwise authorized by Covered Entity.

2.2 ***Use Safeguards***. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement. In accordance with 164.502(e)(1)(ii), to ensure that subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same restrictions and conditions that apply to the BA with respect to such information. Business Associate will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Health Information Business Associate creates, receives, maintains or transmits on behalf of Covered Entity.

2.3 **Mitigate Harmful Effects**. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

2.4 ***Report Impermissible Disclosures of PHI***. Business Associate shall report to Covered Entity a discovery of Breach or any use or disclosure of Protected Health Information not permitted or

required by this Agreement within a reasonable period of time after becoming aware of such use or disclosure, including those occurrences reported to Business Associate by its subcontractors or agents. Business Associate also agrees to report to Covered Entity any Security Incident related to Electronic Protected Health Information of which Business Associate becomes aware.

2.5 ***Report Breach of Unsecured PHI***. In the case of a Breach of Unsecured PHI, Business Associate shall notify Covered Entity as required by 45 CFR §164.410.

2.6 ***Compliance of Agents and Subcontractors***. Business Associate agrees to require any agent, or subcontractor to whom it provides Protected Health Information received from Covered Entity to agree to the same restrictions and conditions that apply to Business Associate through this Agreement with respect to such uses and disclosures of PHI. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect such information, which shall be no less than those required of Business Associate.

2.7 ***Provide Access***. Business Associate agrees to provide access, during normal business hours, to Protected Health Information in a Designated Record Set of Covered Entity to Covered Entity in order to meet the requirements of 45 C.F.R. §164.524, provided Covered Entity delivers written notice to Business Associate at least five business days in advance requesting such access. This provision does not apply if Business Associate and its employees, subcontractors and agents have no Protected Health Information in a Designated Record Set of Covered Entity or if the Protected Health Information held by Business Associate merely duplicates information held by Covered Entity.

2.8 ***Incorporate Amendments***. Business Associate agrees to incorporate any amendment(s) to Protected Health Information in a designated record set of Covered Entity that Covered Entity directs pursuant to 45 C.F.R. §164.526. This provision does not apply if Business Associate and its employees, subcontractors and agents have no Protected Health Information from a designated record set of Covered Entity.

2.9 ***Disclose Practices, Books, and Records***. Unless otherwise protected, or prohibited from discovery or disclosure by law, Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary for purposes of determining Covered Entity's compliance with the Privacy Rule. Business Associate shall have a reasonable time within which to comply with requests for such access and in no case shall access be required in less than five (5) business days after Business Associate's receipt of such request, unless otherwise designated by the Secretary.

2.10 ***Document Disclosures***. Business Associate agrees to maintain sufficient documentation of such disclosures of Protected Health Information by Business Associate as would be required for Covered Entity, or Business Associate on its behalf, to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528.

2.11 ***Accounting of Disclosures***. On request of Covered Entity, Business Associate agrees to provide to Covered Entity, or as directed by Covered Entity, to Individual, an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R.§164.528. Business Associate shall have a reasonable time within which to comply with such a request from Covered Entity and in no case shall Business Associate be required to provide such documentation in less than five (5) business days after Business Associate's receipt of such request.

2.12 ***Respond to Requests from Individuals***. Except as this Agreement or any other agreement between Covered Entity and Business Associate may otherwise provide, in the event Business

Associate receives an access, amendment, accounting of disclosure, or other similar request directly from an Individual, Business Associate will redirect the Individual to Covered Entity.

Section 3
Permitted Uses and Disclosures by Business Associates

3.1 ***Functions and Activities on Behalf of Covered Entity.*** Except as otherwise limited by this Agreement, Business Associate may make any uses and disclosures of Protected Health Information necessary to meet its obligations under this Agreement and under the Contract, if such use or disclosure would not violate the Privacy Rule if done by Covered Entity. All other uses or disclosures by Business Associate not authorized by this Agreement or by specific instruction of Covered Entity are prohibited.

3.2 ***Business Associate's Management and Administration.*** Except as otherwise limited by this Agreement, Business Associate may use Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

3.3 ***Disclosure by Business Associate Required by Law or With Reasonable Assurances.*** Except as otherwise limited by this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate and to carry out its legal responsibilities, provided that disclosure is Required By Law, or provided that the Business Associate obtains reasonable assurances from the person or entity to whom the Protected Health Information is disclosed that: 1) the Protected Health Information will be held confidentially; 2) the Protected Health Information will be used or further disclosed only as Required By Law or for the purpose(s) for which it was disclosed to the person or entity; and 3) the person or entity will notify Business Associate of any instances of which the person or entity is aware in which the confidentiality of the information has been breached.

3.4 ***Data Aggregation Services.*** Except as otherwise limited by this Agreement, Business Associate may use Protected Health Information to provide data aggregation services to Covered Entity as permitted by 45 C.F.R. §164.504(e)(2)(i)(B).

Section 4
Term and Termination

4.1 ***Term.*** The Term of this Agreement shall begin on , or the effective date of the Contract, whichever is later. This Agreement shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created, maintained or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is not feasible in the determination of the Business Associate to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.

4.2 ***Termination for Cause.*** Upon Covered Entity's reasonable determination that Business Associate has breached or violated a material term of this Agreement, Covered Entity shall give Business Associate written notice of such breach and provide reasonable opportunity for Business Associate to cure the breach or end the violation. Covered Entity may terminate the Contract, and Business Associate agrees to such termination, if Business Associate has breached a material term of this Agreement and does not cure the breach or cure is not possible.

4.3 ***Effect of Termination*.** Upon termination of the Contract and receipt of written demand from Covered Entity, Business Associate agrees to, if feasible, return or destroy all Protected Health Information received from, or created or maintained by Business Associate on behalf of, Covered Entity. In the event the return or destruction of such Protected Health Information is not feasible in the determination of Business Associate, the protections of this Agreement will remain in force and Business Associate shall make no further uses and disclosures of Protected Health Information except for the proper management and administration of its business or to carry out its legal responsibilities or as Required By Law.

Section 5
Limitation of Liability

Business Associate's total liability under this Agreement and any other agreement entered into between the parties and any duty to indemnify shall be for direct damages only and should not exceed the professional services fee paid to Business Associate in the preceding thirty (30) days relating to the services to which the liability relates. Business Associate shall not be liable for incidental, consequential, punitive, or exemplary damages, regardless of whether Business Associate was advised of the possibility of such damages. Covered Entity may recover direct damages against Business Associate up to the limits set forth in this Section 5.

Section 6
Miscellaneous Provisions

6.1 ***Regulatory References*.** A reference in this Agreement to a section in the Privacy Rule, Security Rule and HITECH means the Section in effect or as amended and for which compliance is required.

6.2 ***Amendment*.** Business Associate agrees to take such action as is necessary to amend this Agreement from time to time as is necessary, as determined by Business Associate, for Covered Entity to comply with the requirements of the HIPAA Privacy Rule, Security Rule and HITECH.

6.3 ***Survival*.** The rights and obligations of Business Associate under Section 4.3 of this Agreement shall survive the termination of this Agreement and the termination of the Contract.

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

6.5 **Conflicts**. In the event of any discrepancies between the terms of the BAA and the Master Services Agreement, the terms of this BAA shall govern. Absent a discrepancy, the terms of the Master Services Agreement shall apply to the BAA.