

## **Business Associate Addendum**

This Business Associate Addendum (“Addendum”) supplements and is made part of that certain agreement (“Agreement”), which incorporates this Addendum by reference, by and between HealthTech Solutions Group, LLC<sup>®</sup> and Contracting Entity (as defined in the Agreement).

The parties incorporate this Addendum into the Agreement in order to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) (“ARRA”) and their implementing regulations set forth at 45 C.F.R. Parts 160 and 164 (the “Privacy and Security Rule”). To the extent either party is acting as a Business Associate (“Associate”) of the other party and/or the other party’s customers or clients (each, as applicable, an “Entity”) pursuant to the Agreement, the provisions of this Addendum shall apply and Associate shall be subject to the penalty provisions as specified by ARRA (42 USC §§ 17931(c), 17934(c)). To the extent Associate is to carry out an obligation of a Covered Entity under the Privacy and Security Rule, Associate shall comply with the requirements of the Privacy and Security Rule that apply to Covered Entities in the performance of such obligation.

1. **Definitions.** Capitalized terms not otherwise defined in this Addendum shall have the meaning set forth in the Privacy and Security Rule. References to “PHI” mean Protected Health Information created or received by Associate from Entity or on Entity’s behalf.
2. **Uses or Disclosures.** Associate will neither use nor disclose PHI except as permitted or required by this Addendum or as Required by Law. Associate will not sell PHI or use or disclose PHI for purposes of marketing or fundraising, as defined and proscribed in the Privacy and Security Rule and ARRA. Associate is permitted to use and disclose PHI:
  - (i) to perform any and all obligations of Associate as described in the Agreement, provided that such use or disclosure would not violate the Privacy and Security Rule, if done by Entity directly;
  - (ii) as otherwise permitted by law, provided that such use or disclosure would not violate the Privacy and Security Rule, if done by Entity directly and provided that Entity gives its prior written consent;
  - (iii) to perform Data Aggregation services relating to the health care operations of Entity;
  - (iv) to report violations of the law to federal or state authorities consistent with 45 C.F.R. § 164.502(j)(1);
  - (v) as necessary for Associate’s proper management and administration and to carry out Associate’s legal responsibilities (collectively “Associate’s Operations”), provided that Associate may only disclose PHI for Associate’s Operations if the disclosure is Required By Law or Associate obtains reasonable assurance, evidenced by a written contract, from the recipient that the recipient will: (1) hold

such PHI in confidence and use or further disclose it only for the purpose for which Associate disclosed it to the recipient or as Required By Law; and (2) notify Associate of any instance of which the recipient becomes aware in which the confidentiality of such PHI was breached;

- (vi) to de-identify PHI in accordance with 45 C.F.R. § 164.514(b), provided that such de-identified information may be used and disclosed only consistent with applicable law.

In the event Entity notifies Associate of a restriction request that would restrict a use or disclosure otherwise permitted by this Addendum, Associate shall comply with the terms of the restriction request.

3. **Information Safeguards.** Associate will maintain appropriate administrative, technical and physical safeguards to prevent use or disclosure of PHI not permitted by this Addendum. Associate will also maintain administrative, technical and physical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI in compliance with the Privacy and Security Rule.
4. **Subcontractors and Agents.** Associate will require any of its subcontractors and agents, to which Associate discloses any PHI, to agree to comply with the same privacy and security obligations as Associate with respect to such PHI.
5. **Minimum Necessary.** Associate represents that the PHI requested, used or disclosed by Associate shall be the minimum amount necessary to carry out the purposes of the Agreement. Associate will limit its uses and disclosures of, and requests for, PHI (i) when practical, to the information making up a Limited Data Set; and (ii) in all other cases subject to the requirements of 45 CFR § 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.
6. **Obligations of Entity.** Entity shall (i) provide Associate with a copy of the notice of privacy practices that Entity produces pursuant to 45 C.F.R. § 164.520, and Entity shall promptly furnish Associate with copies of any material changes to such notice; (ii) notify Associate of any changes in, or revocation of, permission by an individual to use or disclose PHI, if such changes affect Associate's permitted or required uses or disclosures; (iii) notify Associate of any confidential communication request or restriction to the use or disclosure of PHI affecting Associate that Entity has agreed to in accordance with 45 C.F.R. § 164.522.
7. **Access and Amendment.** Associate shall permit Entity or, at Entity's request, an individual (or the individual's personal representative) to inspect and obtain copies of any PHI about the individual that is in Associate's custody or control and that is maintained in a Designated Record Set. Associate will, upon receipt of notice from Entity, promptly amend or permit Entity access to amend any portion of PHI so that Entity may meet its amendment obligations under 45 C.F.R. § 164.526.
8. **Disclosure Accounting.** Except for disclosures excluded from the accounting obligation by the Privacy and Security Rule and regulations issued pursuant to ARRA, Associate

will record for each disclosure that Associate makes of PHI the information necessary for Entity to make an accounting of disclosures pursuant to the Privacy and Security Rule. Associate will make this information available to Entity promptly upon Entity's request for the period requested, but for no longer than the six (6) years preceding Entity's request for the information (except Associate need not have any information for disclosures occurring before the effective date of this Addendum or with respect to disclosures required to be recorded by ARRA, the effective date of the ARRA regulations with respect to Entity).

9. **Inspection of Books and Records.** Associate will make its internal practices, books, and records, relating to its use and disclosure of PHI, available upon request to Entity or the Secretary of U.S. Department of Health and Human Services ("HHS") to determine Entity's compliance with the Privacy and Security Rule.
10. **Reporting.** To the extent known to or discovered by Associate, Associate shall promptly report to Entity any use or disclosure of PHI not permitted by this Addendum, any Security Incident involving electronic PHI, and any Breach of Unsecured Protected Health Information. Associate shall mitigate, to the extent practicable, any harmful effect known to it of a Security Incident, Breach or use or disclosure of PHI by Associate not permitted by this Addendum. Notwithstanding the foregoing, the parties acknowledge and agree that this section constitutes notice by Associate to Entity of the ongoing existence and occurrence of Deminimus Incidents (as defined below) for which no additional notice to Entity shall be required. "Deminimus Incidents" means (i) attempted but unsuccessful security incidents, including, but not be limited to, pings and other broadcast attacks on Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of electronic PHI; and (ii) incidents involving the incidental access to, or minimal encounter, with PHI provided that the recipient would not reasonably be able to retain such PHI and the incident does not pose a significant risk of harm to the individual who is the subject of the PHI, as reasonably determined by Associate. All reports of Breaches shall be made in compliance with 45 CFR § 164.410.
11. **Term and Termination.**
  - 11.1 **Term.** This Addendum shall be effective as of the effective date of the Agreement and shall remain in effect until termination of the Agreement. Either party may terminate this Addendum and the Agreement effective immediately if it determines that the other party has breached a material provision of this Addendum and failed to cure such breach within thirty (30) days of being notified by the other party of the breach. If the non-breaching party determines that cure is not possible, such party may terminate this Addendum and the Agreement effective immediately upon written notice to other party. If termination is not feasible, the non-breaching party shall report the breach to HHS.
  - 11.2 **Obligations upon Termination.** Upon termination of this Addendum for any reason, Associate will, if feasible, return to Entity or destroy all PHI maintained

by Associate in any form or medium, including all copies of such PHI. Further, Associate shall recover any PHI in the possession of its agents and subcontractors and return to Entity or destroy all such PHI. In the event that Associate determines that returning or destroying any PHI is infeasible, Associate may maintain such PHI but shall continue to abide by the terms and conditions of this Addendum with respect to such information and shall limit its further use or disclosure of such information to those purposes that make return or destruction of the information infeasible.

11.3 Survival. Upon termination of this Addendum for any reason, all of Associate's obligations under this Addendum shall survive termination and remain in effect (a) until Associate has completed the return or destruction of PHI as required by Addendum Section 11.2 and (b) to the extent Associate retains any PHI pursuant to Addendum Section 11.2.

12. General Provisions. In the event that any law, final regulation or amendment to final regulations is promulgated by HHS or other government regulatory authority with respect to PHI or is enacted by legislative authority, the parties shall negotiate in good faith to amend this Addendum to remain in compliance with such law and/or regulations. In the absence of any such amendment, this Addendum shall be amended as a matter of law to conform to the requirements of law. Any ambiguity in this Addendum shall be resolved to permit Entity to comply with the Privacy and Security Rule. Nothing in this Addendum shall be construed to create any rights or remedies in any third parties or any agency relationship between the parties. A reference in this Addendum to a section in the Privacy and Security Rule means the section as in effect or as amended. The terms and conditions of this Addendum override and control any conflicting term or condition of the Agreement. All non-conflicting terms and conditions of the Agreement remain in full force and effect.