



BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

The terms of this Business Associate Subcontractor Agreement (“**BAA**”) are incorporated into and made a part of any Agreement between you, or the entity you represent (“**Subcontractor**”), and Sterling Computers Corporation (each individually referred to as a “**Party**” and collectively as the “**Parties**”), where the Agreement anticipates that you will receive, maintain, create, or transmit Protected Health Information as a subcontractor for Sterling.

1. DEFINITIONS.

- (a) The following terms used in this BAA shall have the same meaning as applied in the HIPAA Rules: Breach, Breach Notification, Data Aggregation, Designated Record Set, De-Identified Information, Disclosure (or Disclose), Electronic Protected Health Information, Electronic Transactions Rule, Enforcement Rule, Genetic Information, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (“**PHI**”), Required By Law, Sale, Secretary, Security Incident, Security Rule, Transaction, Unsecured Protected Health Information, and Use.
- (b) “**Agreement**” means a statement of work, purchase order, or other document describing the Services to be provided by Subcontractor to Sterling’s client on Sterling’s behalf.
- (c) “**Business Associate**” has the same meaning as the term "Business Associate" at 45 C.F.R. § 160.103, and includes Subcontractor with respect to this BAA.
- (d) “**HIPAA**” means the Health Insurance Portability and Accountability Act of 1996, as amended by the HITECH Act, and the related regulations promulgated by the U.S. Department of Health and Human Services.
- (e) “**Covered Entity**” has the same meaning as the term "Covered Entity" at 45 C.F.R. § 160.103.
- (f) “**HIPAA Rules**” means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164. A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended at the time the section is to be applied.
- (g) “**HITECH Act**” means the Health Information Technology for Economic and Clinical Health Act.
- (h) “**Service(s)**” means the service offering or work to be performed by Subcontractor set forth in an applicable statement of work, purchase order, or other agreement between Sterling and Subcontractor.
- (i) “**Subcontractor**” has the same meaning as the term "Subcontractor" at 45 C.F.R. § 160.103, and in this context refers to you as a subcontractor that will provide Services to a Covered Entity, as defined at 45 C.F.R. § 160.103, on behalf of Sterling.
- (j) The following terms used in this BAA have the same meaning as those terms in the HIPAA Rules: Breach, Breach Notification, Data Aggregation, Designated Record Set, De-Identified Information, Disclosure (Disclose), Electronic Protected Health Information, Electronic Transactions Rule, Enforcement Rule, Genetic Information, Health Care Operations,



BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required By Law, Sale, Secretary, Security Incident, Security Rule, Subcontractor, Transaction, Unsecured Protected Health Information, and Use.

2. OBLIGATIONS AND ACTIVITIES OF SUBCONTRACTOR.

Subcontractor shall:

- (a) not Use or Disclose Protected Health Information other than as permitted or required by the Agreement, this BAA, or as Required by Law;
- (b) comply with applicable provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA Act"), the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services ("HIPAA Rules")
- (c) maintain a HIPAA compliance program in compliance with HIPAA Rules and applicable law that includes specific policies and procedures, workforce training, and documentation requirements relating to Protected Health Information and permit Sterling, at its own expense and upon reasonable advanced notice, to review or audit such compliance program and all documentation relating to the Services;
- (d) implement a Common Security Framework, which supports HIPAA requirements with other recognized standards such as NIST and ISO, to provide a certifiable framework for managing regulatory compliance and risk management;
- (e) use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic Protected Health Information, to prevent Use or Disclosure of Protected Health Information other than as provided for by this BAA;
- (f) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI, as required by the Security Rule;
- (g) report to Sterling and, in coordination with Sterling, to the Covered Entity any Use or Disclosure of Covered Entity's Protected Health Information not provided for by the Agreement of which it becomes aware, including Breaches of Unsecured Protected Health Information as required at 45 C.F.R. § 164.410;
- (h) ensure that any other subcontractor that Subcontractor retains to create, receive, maintain, or transmit Protected Health Information on behalf of Subcontractor agrees in writing to the same restrictions, conditions, and requirements that apply to Subcontractor with respect to such Protected Health Information, in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii), 164.308(b)(2), and this BAA, if applicable;
- (i) make available Protected Health Information in a Designated Record Set to Sterling, or Covered Entity if directed by Sterling, as necessary to satisfy Covered Entity's obligations



BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

under 45 C.F.R. § 164.524, including furnishing an electronic copy of Protected Health Information that is maintained in a Designated Record Set;

- (j) make any amendment(s) to Protected Health Information in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. § 164.526 (or by Sterling on the Covered Entity's behalf), or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526;
- (k) maintain and make available the information required to provide an accounting of Disclosures to Sterling and Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.528;
- (l) to the extent Subcontractor is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164 ("Privacy of Individually Identifiable Health Information"), comply with the requirements of such Subpart E that apply to the Covered Entity in the performance of such obligation(s);
- (m) make its internal practices, books, and records available to the Secretary of the Department of Health and Human Services for purposes of determining compliance with the HIPAA Rules;
- (n) not participate in any Sale of Protected Health Information;
- (o) not Use or Disclose Genetic Information for underwriting purposes in violation of the HIPAA Rules;
- (p) comply with the Electronic Transaction Rule and any applicable corresponding requirements adopted by the U.S. Department of Health and Human Services with respect to any Electronic Transactions conducted by Subcontractor on behalf of the Covered Entity in connection with the Services; and
- (q) maintain the confidentiality of Protected Health Information in accordance with confidentiality obligations under HIPAA Rules;

3. PERMITTED USES AND DISCLOSURES BY SUBCONTRACTOR. Subcontractor shall not Use or Disclose Protected Health Information relating to Covered Entity, except as expressly permitted under and consistent with this Section 3.

- (a) Subcontractor may Use or Disclose Protected Health Information only to fulfill its obligations under the Agreement between Sterling and Subcontractor:
- (b) Subcontractor may Use or Disclose Protected Health Information as Required by Law.
- (c) Subcontractor shall not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Sterling, except for the specific Uses and Disclosures set forth in the following provisions of this Section 4.
- (d) Subcontractor may Disclose Protected Health Information for the proper management and administration of Subcontractor or to carry out the legal responsibilities of Subcontractor, provided the Disclosures are Required by Law, or Subcontractor obtains reasonable



BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

assurances from the person to whom the information is Disclosed that the information will remain confidential and Used or further Disclosed only as Required by Law or for the purposes for which it was Disclosed to the person, and the person will notify Sterling of any instances of which the person becomes aware in which the confidentiality of the information has been Breached.

4. NOTIFICATION OF BREACH. If Subcontractor discovers a Breach of Protected Health Information, Subcontractor shall, following the discovery of the Breach of Unsecured Protected Health Information, notify Sterling in writing and, in coordination with Sterling, the Covered Entity of such Breach in accordance with this Section 6.

- (a) Subcontractor shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of Subcontractor.
- (b) Subcontractor shall provide the notification required under this Section 6 without unreasonable delay and in no case later than five calendar days after the discovery of the Breach.
- (c) The notification shall include, to the extent possible, the identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Subcontractor to have been, accessed, acquired, used, or disclosed during the Breach.
- (d) Subcontractor shall provide to Sterling (and, if so requested) to the Covered Entity with any other available information that the Covered Entity is required to include in notification to the individual under 45 C.F.R. § 164.404(c) at the time of the notification by Subcontractor, and any information that is not then available promptly after such information becomes available. Information to be provided includes, to the extent possible:
 - (i) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
 - (ii) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 - (iii) Any steps individuals should take to protect themselves from potential harm resulting from the Breach;
 - (iv) A brief description of what Subcontractor is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and
 - (v) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web site, or postal address.



BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

5. TERM AND TERMINATION

- (a) The term of this BAA will start as of the Effective Date of the Agreement and will continue coterminous with the Agreement, unless Sterling terminates for cause as authorized in clause (b) of this Section 8, whichever is sooner.
- (b) Sterling may terminate this BAA if Sterling reasonably determines in good faith that Subcontractor has violated a material term and Subcontractor has not cured the Breach or ended the violation to the satisfaction of Sterling within 15 days of notice or such longer time period agreed to in writing by Sterling.
- (c) Except as provided in clause (d) of this Section 8, upon termination of this BAA for any reason, Subcontractor shall return to Sterling or, if so directed, to Covered Entity (or, if directed by Sterling in coordination with the Covered Entity, destroy) all Protected Health Information created, maintained, or received by Subcontractor on behalf of the Covered Entity that the Subcontractor still maintains in any form. Subcontractor shall retain no copies of the Protected Health Information.
- (d) If so directed by Sterling, Subcontractor shall transmit any Protected Health Information created, maintained, or received by Subcontractor on behalf of Covered Entity to Sterling, to another Business Associate of the Covered Entity, or to the Covered Entity at termination.
- (e) Subcontractor shall be responsible for compliance with the obligations regarding the Covered Entity's Protected Health Information described in this Section 8 with respect to any applicable Protected Health Information that is created, received, or maintained by any other Subcontractors retained by Subcontractor.
- (f) The obligations of Subcontractor under this Section 8 shall survive the termination of this BAA.

- 6. INDEMNIFICATION; INSURANCE.** Subcontractor agrees to indemnify, defend, and hold harmless Sterling and its employees, directors, officers, representatives, and agents (collectively, the "Indemnitees") from and against any and all claims, obligations, actions, suits, debts, judgments, losses, fines, penalties, damages, costs, expenses (including reasonable attorney's fees), and other liabilities ("Covered Liabilities") incurred by the Indemnitees that arise or result from a breach of the terms and conditions of this BAA or a violation of applicable law by Subcontractor or its employees, contractors, or agents; provided, however, that (A) Covered Liabilities shall exclude consequential, special, and punitive damages), and (B) the indemnification rights hereunder are conditioned on (i) Sterling giving the Subcontractor prompt written notice of any Covered Liability; (ii) Sterling providing commercially reasonable cooperation in the defense or mitigation of a Covered Liability, if reasonably requested by Subcontractor (with Subcontractor bearing any additional expense to Sterling); and (iii) Sterling not entering into any settlement or compromise in respect of a Covered Liability without Subcontractor's prior written consent, which consent may not be unreasonably withheld or delayed.



BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

7. GENERAL PROVISIONS.

- (a) **Regulatory References.** A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.
- (b) **Amendment.** Sterling may amend this BAA from time to time as necessary to comply with the requirements of the HIPAA Rules and any other applicable law.
- (c) **Interpretation.** Any ambiguity in this BAA should be interpreted to permit the Parties to comply with the HIPAA Rules and other applicable law.
- (d) **Governing Law.** This BAA is governed by the laws of South Dakota, except to the extent preempted by federal law.
- (e) **Severability.** The provisions of this Agreement are severable, and the invalidity of any provision shall not affect the validity of other provisions of this BAA.
- (f) **No Waiver.** No provision of this BAA may be waived except by an agreement in writing signed by the waiving Party. A waiver of any term or provision will not be construed as a waiver of any other term or provision.