



The terms of this Business Associate Agreement (“**BAA**”) apply when Client is a Client or a Business Associate of a Client (as those terms are defined below) and Client engages Sterling Computers Corporation (“**Sterling**”) under one or more Agreements to provide certain specified Offerings and, in providing such Offerings pursuant to such Agreements, Sterling will have access to Protected Health Information.

The terms of this BAA do not apply when Client is neither a Covered Entity nor a Business Associate of a Covered Entity.

1. DEFINITIONS.

- 1.1. “**Agreement**” means a statement of work, purchase order, or other document describing the Offerings to be provided by Sterling to Client.
- 1.2. “**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.
- 1.3. “**HIPAA Rules**” means the following portions of HIPAA: (i) the Privacy Rule set forth at 45 CFR Part 160 and Part 164, Subparts A and E; (ii) the Security Rule set forth at 45 CFR Part 160 and Part 164, Subparts A and C; and (iii) the Breach Notification Rule set forth at 45 CFR Part 164, Subpart D.
- 1.4. “**HITECH Act**” means the Health Information Technology for Economic and Clinical Health Act.
- 1.5. “**Offerings**” means the Sterling-branded Digital Personalities™, and any other product, service, or other offering which Sterling makes generally available to its clients.
- 1.6. **Additional Terms.** The following terms used in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Breach Notification, Business Associate, Client, Data Aggregation, Designated Record Set, De-Identified Information, Disclosure (Disclose), Electronic Protected Health Information (ePHI), 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, Subcontractor, Transaction, Unsecured Protected Health Information, and Use.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.

- 2.1. Sterling will not Use or Disclose PHI other than as permitted or required by this BAA or as Required by Law.
- 2.2. Sterling will use appropriate safeguards, and comply, where applicable, with Subpart C of 45 C.F.R. Part 164 with respect to ePHI, to prevent Use or Disclosure of PHI other than as provided for by the relevant Agreement(s) or this BAA.



- 2.3. Sterling will report to Client any actual Use or Disclosure of PHI not provided for by this BAA of which it becomes aware, including Breaches of Unsecured PHI as required at 45 C.F.R. § 164.410.
 - 2.4. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, Sterling will ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Sterling agree to the same or greater restrictions, conditions, and requirements that apply to Sterling with respect to such information.
 - 2.5. In accordance with 45 CFR 164.524, Sterling will make available PHI as necessary.
 - 2.6. In accordance with 45 CFR 164.526, Sterling will make amendments to PHI and make available PHI for amendments.
 - 2.7. In accordance with 45 CFR 164.528, Sterling will maintain and make available the information required to provide an accounting of Disclosures.
 - 2.8. To the extent Sterling is to carry out one or more of Client's obligation(s) under Subpart E of 45 C.F.R. Part 164 ("Privacy of Individually Identifiable Health Information"), Sterling will comply with the requirements of such Subpart E that apply to the Client in the performance of such obligation(s).
 - 2.9. Sterling will make its internal practices, books, and records relating to the use and disclosure of PHI received from Client (or created or received by Sterling on behalf of Client) available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with the HIPAA Rules.
 - 2.10. Sterling will not participate in any Sale of PHI.
- 3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.**
- 3.1. Sterling may Use and Disclose PHI to provide the Offerings to Client, to perform its duties, obligations, and functions under the relevant Agreement(s), or as otherwise permitted or required by the relevant Agreement(s) or this BAA.
 - 3.2. Sterling may Use and Disclose PHI for the proper management and administration of Sterling.
 - 3.3. In accordance with 42 CFR 164.514(b), Sterling may de-identify any and all PHI. The Parties understand that properly De-Identified Information is not PHI under the terms of this BAA.
 - 3.4. Sterling may Use or Disclose PHI as Required by Law.
 - 3.5. Sterling will implement appropriate safeguards to prevent Use or Disclosure of PHI. Sterling may Use PHI to carry out its legal responsibilities.
 - 3.6. Sterling may Use PHI to provide Data Aggregation services relating to the Health Care Operations of Client.



4. PROVISIONS FOR CLIENT TO INFORM STERLING OF PRIVACY PRACTICES AND RESTRICTIONS.

- 4.1. Client shall notify Sterling of any limitation(s) in the Notice of Privacy Practices of Client under 45 C.F.R. § 164.520, to the extent that such limitation may affect Sterling's Use or Disclosure of PHI.
- 4.2. Client shall notify Sterling of any changes in, or revocation of, the permission by an individual to Use or Disclose his or her PHI, to the extent that such changes may affect Sterling's Use or Disclosure of PHI.
- 4.3. Client shall notify Sterling of any restriction on the Use or Disclosure of PHI that Client has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect Sterling's Use or Disclosure of PHI.

5. NOTIFICATION OF BREACH. If Sterling discovers a Breach of PHI, Sterling shall, following the discovery of the Breach of Unsecured PHI, notify the Client of such Breach in accordance with this Section 6.

- 5.1. Sterling 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 Sterling.
- 5.2. Sterling shall provide the notification required under this Section 6 without unreasonable delay and in no case later than five calendar days after discovery of the Breach.
- 5.3. The notification shall include, to the extent possible, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Sterling to have been, accessed, acquired, used, or disclosed during the Breach.
- 5.4. Sterling shall provide the Client with any other available information that the Client is required to include in notification to the individual under 45 C.F.R. § 164.404(c) at the time of the notification by Sterling, and any information that is not then available promptly after such information becomes available. Information to be provided includes, to the extent possible:
 - 5.4.1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
 - 5.4.2. A description of the types of Unsecured PHI 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); and
 - 5.4.3. A brief description of what Sterling is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches.



6. **PERMISSIBLE REQUESTS BY CLIENT.** Client shall not request Sterling to Use or Disclose PHI in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by Client.

7. **TERM AND TERMINATION**

- 7.1. **Term.** The term of this BAA shall be effective as of the Effective Date of the Agreement and shall continue coterminous with the Agreement, unless terminated earlier for cause as set forth in paragraph (b) of this Section 8.
- 7.2. **Termination for Cause.** Client may terminate this BAA if it reasonably determines in good faith that Sterling has violated a material term of this BAA and Sterling has not cured the Breach or ended the violation to the reasonable satisfaction of Client within 15 days or such longer time period specified by Client. Sterling may terminate this BAA if it reasonably determines in good faith that Client has violated a material term of the Agreement or this BAA and Client has not cured the Breach or ended the violation to the reasonable satisfaction of Sterling within 15 days or such longer time period agreed to in writing by Sterling.
- 7.3. **Obligations of Business Associate Upon Termination.** Except as set forth in Section 8(d), upon termination of this BAA for any reason, Sterling, with respect to PHI received from Client, or created, maintained, or received by Sterling on behalf of Client, shall:
- 7.3.1. retain only that PHI which is necessary for Sterling to continue its proper management and administration or to carry out its legal responsibilities;
- 7.3.2. return to Client (or, if agreed to by Client, destroy) the remaining PHI that Sterling still maintains in any form;
- 7.3.3. continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI to prevent Use or Disclosure of the PHI, other than as provided for in this Section, for as long as Sterling retains PHI;
- 7.3.4. not Use or Disclose the PHI retained by Sterling other than for the purposes for which such PHI was retained and subject to the same conditions set out in this BAA which applied prior to termination; and
- 7.3.5. return to Client (or, if agreed to by Client, destroy) the PHI retained by Sterling when it is no longer needed by Sterling for its proper management and administration or to carry out its legal responsibilities.
- 7.4. **Transmission of Protected Health Information.** If so directed by Client, Sterling shall transmit any PHI received from Client, or created, maintained, or received by Sterling on behalf of Client, to another [Business Associate/Subcontractor] of Client at termination.
- 7.5. **Subcontractors.** Sterling will ensure that any of its agents or subcontractors that have access to, or to which Sterling provides, PHI agree in writing to the restrictions and conditions concerning Use and Disclosure of PHI contained in this BAA and agree to



implement reasonable and appropriate safeguards to protect any Electronic PHI that they create, receive, maintain or transmit on behalf of Sterling.

8. GENERAL PROVISIONS.

- 8.1. **Regulatory References.** A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended, and for which compliance by a Party is required.
- 8.2. **Interpretation.** Any ambiguity in this BAA shall be interpreted to permit the Parties to comply with the HIPAA Rules and other applicable law.
- 8.3. **Governing Law.** This BAA shall be governed by the laws of South Dakota, except to the extent preempted by federal law.
- 8.4. **Severability.** The provisions of this BAA are severable, and the invalidity of any provision shall not affect the validity of other provisions of this BAA.
- 8.5. **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 shall not be construed as a waiver of any other term or provision.
- 8.6. **Notice.** Any notice required under this BAA must be in writing and delivered by electronic mail to the address of the Party specified in the Agreement or such other address as either Party may specify in writing.