Bonterms Standard Agreement
Business Associate Agreement (BAA)
(Version 1.0)

This Bonterms Business Associate Agreement (Version 1.0) ("**BAA**") is a set of standard terms entered into between Business Associate and Customer by executing a Cover Page.

1. Definitions.

1.1. "**Breach**", "**Covered Entity**", "**Designated Record Set**", "**Disclosure**", "**Individual**", "**Required by Law**", "**Secretary**", "**Security Incident**", "**Unsecured PHI**", "**Use**", and any other terms defined in the HIPAA Rules, whether capitalized or not, have the meaning ascribed to such terms in the HIPAA Rules unless otherwise specified.

1.2. "**Additional Terms**" means any additions to or modifications of this BAA that the parties specify on a Cover Page.

1.3. "**Business Associate**" is identified on the Cover Page.

1.4. "**BAA Effective Date**" is specified on the Cover Page.

1.5. "**Cover Page**" means a separate document executed by Customer and Business Associate which specifies the Key Terms and any Additional Terms and causes them to enter into this BAA.

1.6. "**Customer**" is identified on the Cover Page.

1.7. "**Data Disposition Period**" is defined in Section 5.2.

1.8. "**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, and implementing regulations.

1.9. "**HIPAA Rules**" means the Privacy Rule and Security Rule.

1.10. "**HITECH Act**" means the Health Information Technology for Economic and Clinical Health Act, codified at 42 U.S.C. §§ 17921–17954, and implementing regulations.

1.11. "**HHS**" means the Department of Health and Human Services.

1.12. "**Key Terms**" means the BAA Effective Date and Main Agreement.

1.13. "**Main Agreement**" means the separate agreement under which Business Associate is providing a service to Customer to which this BAA relates.

1.14. "**Privacy Rule**" means the standards for permissible uses and disclosures of Protected Health Information codified at 45 C.F.R. Part 160 and Subparts A and E of Part 164.

1.15. "**Protected Health Information**" or "**PHI**" means protected health information or electronic protected health information (as such terms are defined in the HIPAA Rules) that Business Associate creates, receives, maintains, or transmits on behalf of Customer in connection with activities under the Main Agreement.

1.16. "**Response Period**" means ten days.

1.17. "**Safeguards**" is defined in Section 3.2(a).

1.18. "**Security Incident**" is defined in the HIPAA Rules.

1.19. "**Security Rule**" means the standards for security of Protected Health Information codified at 45 C.F.R. Part 160 and Subparts A and C of Part 164.

1.20. "**Subcontractor**" is defined in Section 3.7.

1.21. "**Unsuccessful Security Incident**" means an attempted but failed Security Incident involving PHI or a Business Associate's information system containing PHI, such as pings or other broadcast attacks on a firewall, denial of service attacks, port scans, or unsuccessful login attempts, or interception of encrypted information where the key is not compromised, or any combination of the above.

2. Role of the Parties. Business Associate provides a service to Customer under the **Main Agreement** which may involve creating, receiving, maintaining, or transmitting PHI.

3. Obligations of Business Associate.

3.1. Permitted Uses and Disclosures of PHI.

(a) Business Associate may Use and Disclose PHI to perform functions, activities, or services for, or on behalf of, Customer as specified in the Main Agreement.

(b) Business Associate agrees not to Use or Disclose PHI other than as permitted or required by the Main Agreement, this BAA, or as Required by Law.

(c) Business Associate may Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

(d) Business Associate may Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that (i) such disclosure was Required by Law or (ii) Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose of which it was Disclosed, and the person notifies Business Associate of any instances of which it is aware where confidentiality of the information has been breached.

3.2. Adequate Safeguards for PHI.

(a) Business Associate will implement and maintain appropriate safeguards designed to prevent the Use or Disclosure of PHI in any manner other than as permitted by this BAA ("**Safeguards**").

(b) Safeguards will include administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any PHI that Business Associate creates, receives, maintains, or transmits on behalf of Customer.

(c) Business Associate will comply with the Security Rule as applicable to Business Associate.

3.3. Event Reporting Obligations.

(a) *Unauthorized Use or Disclosure*. Business Associate will report to Customer any Use or Disclosure of PHI by Business Associate (including its employees or Subcontractors) not permitted under this BAA of which it becomes aware without unreasonable delay, but no later than the Response Period following Business Associate becoming aware of such Use or Disclosure.

(b) *Security Incidents*. Business Associate will report to Customer any Security Incident affecting PHI of which it becomes aware without unreasonable delay, but no later than the Response Period following Business Associate becoming aware of the Security Incident. For Unsuccessful Security Incidents, notice is deemed provided and no further notice will be required.

(c) *Breach of Unsecured PHI.*

(i) Business Associate will report to Customer any Breach of Unsecured PHI ("**Breach Report**") of which it becomes aware without unreasonable delay, but no later than the Response Period following Business Associate becoming aware of the Breach of Unsecured PHI.

(ii) Each Breach Report, to the extent possible, will include the identification of each Individual whose Unsecured PHI has been or is reasonably believed to have been Breached and other information regarding the Breach as reasonably requested by Customer.

(iii) Business Associate will (A) supplement its Breach Report if the above information is not available at the time of the initial report and (B) otherwise cooperate with Customer's requests for information as may be necessary for Customer to evaluate the scope of the Breach and related compliance issues.

3.4. Availability of Internal Records to Government Agencies.

(a) Business Associate will make its internal practices, books, and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining Customer's compliance with the HIPAA Rules.

(b) Business Associate will, if permitted by law, promptly notify Customer of any requests made by the Secretary relating to Customer and provide Customer with copies of any documents produced in response to such request.

3.5. Access to and Amendment of PHI. Within the Response Period following a request by Customer, Business Associate will make PHI in a Designated Record Set available to Customer to enable Customer to make access available to an Individual, make amendments and incorporate such amendments into the PHI, or otherwise fulfill its obligations under the Privacy Rule (including, but not limited to, 45 C.F.R. Section 164.524 and 164.526).

3.6. Accounting of Disclosures. Business Associate will document Business Associate's Disclosures of PHI and provide such information to Customer as necessary to permit Customer to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR Section 164.528 and Section 13405(c) of Title XII, Subtitle D of the HITECH Act.

3.7. Subcontractors. Business Associate may Disclose PHI to one or more subcontractors (each, a "**Subcontractor**"), and may allow a Subcontractor to create, receive, maintain, or transmit PHI on its behalf, provided that Business Associate executes a written agreement obligating each such Subcontractor to comply with the same restrictions and conditions that apply to Business Associate with respect to the PHI.

3.8. Agreement to Mitigate. Business Associate will 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 this BAA.

3.9. Compliance with Customer Obligations. To the extent Business Associate carries out Customer's obligations under the Privacy Rule, Business Associate will comply with the requirements of such Privacy Rule that apply to Customer in the performance of such obligations.

3.10. Minimum Necessary. Business Associate will Use or Disclose the minimum necessary amount of PHI to accomplish the purposes of the Use or Disclosure in accordance with the HIPAA Rules.

3.11. HITECH Act Compliance. Business Associate will comply with the requirements of the HITECH Act which are applicable to business associates.

4. Obligations of Customer.

4.1. Safeguards. Customer is responsible for implementing appropriate privacy and security safeguards, including the privacy and security safeguards required of Customer under the **Main Agreement**, in order to protect its PHI in accordance with the HIPAA Rules.

4.2. Notice of Privacy Practices. Customer will inform Business Associate of any limitation in its notice of privacy practices adopted in accordance with the Privacy Rule, to the extent that such limitation may affect Business Associate's Use or Disclosure of PHI.

4.3. Information on Restrictions. Customer will inform Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI if such changes affect Business Associate's Use or Disclosure of PHI.

4.4. Impermissible Requests. Customer will not request or cause Business Associate to Use or Disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Customer.

5. Term and Termination.

5.1. Duration of BAA. This BAA commences on the **BAA Effective Date** and terminates upon expiration or termination of the **Main Agreement**.

5.2. Disposition of PHI Upon Termination or Expiration. Within 60 days after expiration or earlier termination of this BAA ("**Data Disposition Period**"), Business Associate will, if feasible, return or destroy all PHI it still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of this BAA and limit further Uses and Disclosures of such PHI to those purposes that make the deletion infeasible.

6. General Terms.

6.1. Order of Precedence. The Cover Page will control in any conflict with this BAA.

6.2. Relationship to Main Agreement.

(a) By executing a Cover Page and entering into this BAA, the parties incorporate this BAA (including the Cover Page) into the **Main Agreement**.

(b) If a provision of this BAA (including the Cover Page) is contrary to a provision of the **Main Agreement**, the provision of this BAA will control. Otherwise, this BAA will be construed under, and in accordance with, the terms of the **Main Agreement**.

(c) The parties acknowledge that any liability provisions of the Main Agreement apply to this BAA.

6.3. No Third-Party Beneficiaries. There are no third-party beneficiaries to this BAA.

6.4. Independent Contractors. The parties are independent contractors, not agents, partners, or joint venturers. Neither party will represent itself as the agent or legal representative of the other for any purpose.