

HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement (the “Business Associate Agreement”) is made effective as of the Effective Date by and between DataHEALTH, Inc. and the Customer that entered into the Terms of Service Agreement (the “Agreement”).

RECITALS

Customer is a “Covered Entity” as that term is defined under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the HIPAA administrative simplification regulations, 45 C.F.R. Parts 160 and Part 164, Subparts A, C and E (Subpart E, together with the definitions in Subpart A is known as the “Standards for Privacy of Individually Identifiable Health Information” (the “Privacy Rule”) and Subpart C, together with the definitions in Subpart A, is known as the “Security Standards for the Protection of Electronic Protected Health Information” (the “Security Rule”) (the Privacy Rule and the Security Rule are collectively called the “Privacy and Security Rules”).

Customer and Business Associate are parties to the Agreement under which DataHEALTH provides certain services to Customer. In connection with DataHEALTH’s provision of services to Customer, Customer discloses to DataHEALTH “Protected Health Information” (“PHI”), including “Electronic Protected Health Information” (“ePHI”), as defined in 45 C.F.R. §160.103. Such disclosure results in DataHEALTH’s use, disclosure, maintenance and/or creation of PHI, including ePHI, on behalf of Customer.

DataHEALTH’s provision of services to Customer, when coupled with Customer’s disclosure of PHI to DataHEALTH, makes DataHEALTH a “business associate” of Customer, as the term is defined in as defined in 45 C.F.R. §160.103.

The purpose of this Business Associate Agreement is to comply with the requirements of the Privacy and Security Rules, including, but not limited to, the DataHEALTH Business Associate Agreement requirements at 45 C.F.R. §§ 164.314(a) and 164.504(e), and to satisfy the provisions of the Health Information Technology for Economic and Clinical Health Act, set forth in Division A, Title XIII, of the American Recovery and Reinvestment Act of 2009, and its implementing regulations and guidance (collectively, “HITECH”), including the Omnibus Final Rule, that: (i) affect the relationship between a DataHEALTH and a Customer and which under HITECH and the Omnibus Final Rule require amendments to the DataHEALTH Business Associate Agreement; and (ii) enable Customer to comply with the requirement to notify affected individuals in the event of a Breach of Unsecured Protected Health Information.

Customer’s disclosure of PHI to DataHEALTH, and DataHEALTH’s use, disclosure and creation of PHI for or on behalf of Customer, is subject to protection and regulation under the Privacy Rule. To the extent such use, disclosure or creation involves ePHI, such ePHI is subject to protection and regulation under the Security Rule. DataHEALTH acknowledges it shall comply with the Privacy and Security Rules regarding the use and disclosure of PHI and ePHI, pursuant to this Business Associate Agreement and as required by HITECH and its implementing regulations.

Therefore, Customer and DataHEALTH agree as follows:

1. Definitions.

- (a) Unless otherwise provided in this Business Associate Agreement, capitalized terms have the same meanings as set forth in the Privacy Rule, Security Rule, HITECH, and the Omnibus Final Rule.
- (b) “PHI” means “Protected Health Information,” as that term is defined in the Privacy and Security Rules. “ePHI” means “Electronic Protected Health Information,” as that term is defined in the Privacy and Security Rules. PHI includes PHI that is ePHI as well as PHI that does not constitute ePHI.
- (c) “Unsecured PHI” or “Unsecured Protected Health Information” includes PHI in any form that is not secured through use of a technology or methodology specified in the HITECH, those being: (1) encryption for ePHI in accordance with the appropriate NIST standards for data at rest and in transit; or (2) destruction for other forms of PHI.
- (d) “ePHI” means any PHI that is received, maintained, transmitted or utilized for any purpose in electronic form by DataHEALTH on behalf of Customer.
- (e) “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, as amended by the Stimulus Act; and regulations adopted pursuant thereto, including but not limited to 45 C.F.R. Parts 160 and 164.
- (f) “HITECH Act” means the American Recovery and Reinvestment Act of 2009 (P.L. 111-5), Div. A, Title XIII and Div. B, Title IV, the Health Information Technology for Economic and Clinical Health Act.
- (g) “Omnibus Final Rule” means the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, as published at 78 FR 5565 on January 25, 2013, when and as effective.
- (h) “Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Security Incidents shall not include routine activity such as pings and other broadcast attacks on DataHEALTH's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access to Protected Health Information, or any use or disclosure of Protected Health Information.

2. Scope of Uses and Disclosures by DataHEALTH.

- (a) In General. Except as otherwise limited in this Business Associate Agreement or by law, DataHEALTH may use or disclose PHI provided to DataHEALTH by

Customer to perform the functions, activities, or services for or on behalf of Customer that are specified in the Agreement, provided that such uses or disclosures would not violate the Privacy Rule if done by a Covered Entity or the Minimum Necessary policies and procedures of DataHEALTH.

- (b) Use of PHI. Except as otherwise limited in this Business Associate Agreement or by law, DataHEALTH may use PHI for the proper management and administration of DataHEALTH or to carry out the legal responsibilities of DataHEALTH.
- (c) Disclosure of PHI. Except as otherwise limited in this Business Associate Agreement or by law, DataHEALTH may disclose PHI for the proper management and administration of DataHEALTH or to carry out the legal responsibilities of DataHEALTH, provided that disclosures are required by law, or DataHEALTH obtains reasonable assurances, in writing, from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies DataHEALTH, in writing, within five (5) business days, of any instances of which it is aware in which the confidentiality of the information has been breached.
- (d) Data Aggregation. Except as otherwise limited in this Business Associate Agreement or by law, DataHEALTH may use PHI to provide Data Aggregation services to Customer as permitted by 45 CFR § 164.504(e)(2)(i)(B).
- (e) Limitation on Use and Disclosure of PHI. With regard to its use and/or disclosure of PHI necessary to perform its obligations to Customer, DataHEALTH agrees to limit disclosures of PHI to the Minimum Necessary (as defined in the Privacy Rule, as modified by HITECH and the Omnibus Final Rule) to accomplish the intended purpose of the use, disclosure or request, respectively, whenever the Privacy Rule limits the use or disclosure in question to the Minimum Necessary.
- (f) Limitation on Remuneration for PHI. With regard to its use and/or disclosure of PHI necessary to perform its obligations to Customer and to comply with HITECH and the Omnibus Final Rule, DataHEALTH agrees that it will not receive direct or indirect remuneration for any exchange of PHI not otherwise authorized without individual authorization, unless (i) specifically required for the provision of services under the Agreement (ii) for treatment purposes; (iii) providing the individual with a copy of his or her PHI; or (iv) otherwise determined by the Secretary in regulations.
- (g) Reporting Violation of Law. DataHEALTH may use PHI to report a violation of law to appropriate Federal and/or State authorities, consistent with 45 CFR §164.502(j)(1).

3. Obligations of DataHEALTH.

- (a) In General. DataHEALTH shall use or further disclose PHI only as permitted or required by this Business Associate Agreement or as required by law.

- (b) Safeguards. DataHEALTH shall use reasonable and appropriate safeguards to prevent use or disclosure of PHI other than as specifically authorized by this Business Associate Agreement. Such safeguards shall at a minimum include: (i) a comprehensive written information privacy and security policy addressing the requirements of the Privacy and Security Rules, as amended by HITECH and the Omnibus Final Rule, that are directly applicable to DataHEALTH; and (ii) periodic and mandatory privacy and security training and awareness for members of DataHEALTH's Workforce.
- (c) Mitigation. DataHEALTH shall mitigate any harmful effect that is known to DataHEALTH of a use or disclosure of PHI by DataHEALTH that violates the requirements of this Business Associate Agreement or applicable law.
- (d) Reporting. DataHEALTH shall report to Customer any use or disclosure of PHI that is not sanctioned by this Business Associate Agreement of which DataHEALTH becomes aware within fifteen (15) business days.
- (e) Subcontractors. DataHEALTH shall require subcontractors or agents to whom DataHEALTH provides PHI to agree, in writing, to comply with the Privacy and Security Rules, as amended by HITECH and the Omnibus Final Rule, to the same extent DataHEALTH is required to comply.
- (f) Inspection by Secretary. DataHEALTH shall make available to the Secretary of Health and Human Services DataHEALTH's internal practices, books and records relating to the use and disclosure of PHI for purposes of determining Customer and DataHEALTH's compliance with the Privacy and Security Rules, HITECH, and the Omnibus Final Rule subject to any applicable legal privileges.
- (g) Accounting of Disclosures of PHI. DataHEALTH shall document disclosures of PHI and information related to those disclosures necessary to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with the Privacy Rule, as required by HITECH, and provide to Customer, and in the time and manner it reasonably specifies but in no case longer than fifteen (15) business days, the information necessary to make an accounting of disclosures of PHI about an Individual. If PHI is maintained in an Electronic Health Record ("EHR"), DataHEALTH shall document and maintain documentation of such disclosures as would be required for Customer to respond to a request by an Individual for an accounting of disclosures in an EHR, as required by HITECH.
- (h) Access to PHI. DataHEALTH shall provide to Customer, at Customer's request and in the time and manner it reasonably specifies but in no case longer than fifteen (15) business days, PHI necessary to respond to Individuals' requests for access to PHI about them, in the event that the PHI in DataHEALTH's possession constitutes a Designated Record Set. If PHI is maintained in an Electronic Health Record, DataHEALTH shall provide access electronically, upon reasonable request of Customer.

- (i) Amendment to PHI. DataHEALTH shall, upon receipt of notice from Customer but in no case longer than fifteen (15) business days, incorporate any amendments or corrections to the PHI in accordance with the Privacy Rule, in the event that the PHI in DataHEALTH's possession constitutes a Designated Record Set.
- (j) Security of PHI. DataHEALTH shall, as described in HITECH Act §13401, comply with 45 CFR §§ 164.308, 164.310, 164.312, and 164.316 of the Security Rule and acknowledges that such provisions apply to DataHEALTH in the same manner that they apply to Customer. Therefore, DataHEALTH agrees that it is required to maintain appropriate and reasonable administrative, physical, and technical safeguards, including documentation of the same, so as to ensure that PHI is not used or disclosed other than as provided by this Business Associate Agreement or as required by law, including the following:
 - (i) Administrative safeguards (implementation of policies and procedures to prevent, detect, contain, and correct security violations; conducting and documentation of risk analysis and risk management);
 - (ii) Physical safeguards (implementation of policies and procedures to limit physical access to PHI or ePHI or electronic information systems and related facilities);
 - (iii) Technical safeguards (implementation of policies and procedures creating and tracking unique user identification, authentication processes, and transmission security);
 - (iv) Policies and procedures to reasonably and appropriately document the foregoing safeguards as required by the Security Rule; and
 - (v) Ensuring that any agent, including any subcontractor, to whom DataHEALTH provides ePHI agrees, in writing, to comply with these administrative, physical, and technical safeguards, as well as the policies, procedures, and document requirements contained within the Security Rule.
- (k) Civil and Criminal Liability. DataHEALTH acknowledges that it shall be liable under the civil and criminal enforcement provisions set forth at 42 USC §§1320d-5 and 1320d-6, as amended from time to time, for failure to comply with any use or disclosure requirements of this Business Associate Agreement with respect to PHI and for failure to comply with its direct obligations under the Privacy and Security Rules, HITECH, and the Omnibus Final Rule.
- (l) Notification of Security Incidents and Breach of Unsecured PHI. DataHEALTH shall immediately, but in no case longer than fifteen (15) business days following discovery, notify Customer of any actual or suspected Security Incident or Breach of Unsecured Protected Health Information. The notice shall include: (i) the identification of each Individual whose PHI or Unsecured PHI has been or is reasonably believed by DataHEALTH to have been accessed, acquired, used or disclosed during the Security Incident or Breach, (ii) a brief description of what

happened, including the date of the Security Incident or Breach and the date of the discovery of the Security Incident or Breach, (iii) a description of the types of PHI or Unsecured PHI that were involved in the Security Incident or Breach, (iv) any preliminary steps taken to mitigate the damage, and (v) a description of any investigatory steps taken. In addition, DataHEALTH shall provide any additional information reasonably requested by Customer for purposes of investigating a Breach of Unsecured PHI. A Breach shall be treated as discovered by DataHEALTH as of the first day on which the Breach is known to DataHEALTH (including any person, other than the Individual committing the Breach, that is an employee, officer, or other agent of DataHEALTH) or should reasonably have been known to DataHEALTH to have occurred. Customer shall have the sole right to determine, with respect to a Breach: (i) whether notice is to be provided to Individuals, regulators, law enforcement agencies, consumer reporting agencies, media outlets and/or the Department of Health and Human Services, or others as required by law or regulation, in Customer's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to Individuals affected, and the nature and extent of any such remediation.

4. Obligations of Customer.

- (a) Limitation in Notice of Privacy Practices. Customer will notify DataHEALTH of any limitation in Customer's Notice of Privacy Practices in accordance with the Privacy Rule, to the extent that the limitation may affect DataHEALTH's use or disclosure of PHI.
- (b) Changes in Permission by Individual. Customer will notify DataHEALTH of any changes in, or revocation of, permission by an Individual to use or disclose PHI to the extent that the change may affect DataHEALTH's use or disclosure of PHI.
- (c) Restriction on Use/Disclosure of PHI. Customer will notify DataHEALTH of any restriction on the use or disclosure of PHI that has been agreed to with an Individual and any restrictions on marketing or fundraising to the extent that the restriction may affect DataHEALTH's use or disclosure of PHI.
- (d) Permitted by the Privacy Rule or HITECH. Customer will not request DataHEALTH to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or HITECH if done by a Customer, except to the extent DataHEALTH will use or disclose PHI for, and this Business Associate Agreement includes provisions for, Data Aggregation by or management, administrative, and legal activities of DataHEALTH.

5. Term and Termination.

- (a) Term of the Business Associate Agreement. The term of this Business Associate Agreement begins on the Effective Date and ends when all of the PHI provided to DataHEALTH by Customer, or created or received by DataHEALTH on behalf of Customer, is destroyed or returned to Customer. To the extent it is infeasible for

DataHEALTH to return or destroy the PHI, upon the agreement of Customer, protections shall be extended to that PHI in accordance with the termination provisions in this Section.

- (b) Termination for Breach. Either party may terminate this Business Associate Agreement if it determines that the other party has breached a material term of this Business Associate Agreement. Alternatively, the non-breaching party may choose to provide the breaching party with notice of the existence of an alleged material breach and afford an opportunity to cure the material breach. If the breaching party fails to cure the breach to the satisfaction of the non-breaching party, the non-breaching party may immediately thereafter terminate this Business Associate Agreement.
 - (c) Automatic Termination. This Business Associate Agreement will automatically terminate on the date DataHEALTH ceases to provide to the services described in the in the Agreement
 - (d) Effect of Termination. Upon termination of this Business Associate Agreement, DataHEALTH will return or destroy all PHI received from Customer or created or received by DataHEALTH on behalf of Customer that DataHEALTH still maintains and will retain no copies of that PHI. However, if this return or destruction is not feasible, upon the agreement of Customer, then DataHEALTH will extend the protections of this Business Associate Agreement to the PHI and will limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
6. Business Associate Agreement. Customer and DataHEALTH agree to take any reasonable action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Customer and DataHEALTH to comply with the requirements of the Privacy and Security Rules, HITECH, the Omnibus Final Rule, and any other implementing regulations or guidance.
 7. Interpretation. Any ambiguity in this Business Associate Agreement shall be resolved to permit Customer to comply with the Privacy and Security Rules, HITECH, and the Omnibus Final Rule.
 8. Survival. The obligations of DataHEALTH under Section 5(d) of this Business Associate Agreement survive any termination of this Business Associate Agreement.
 9. No Third Party Beneficiaries. Nothing express or implied in this Business Associate Agreement is intended to confer, nor shall anything in this Business Associate Agreement confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.
 10. Independent Contractor Status. DataHEALTH will be considered, for all purposes, an independent contractor, and DataHEALTH will not, directly or indirectly, act as agent, servant or employee of Customer or make any commitments or incur any liabilities on behalf of Customer without its express written consent. Nothing in this Business Associate

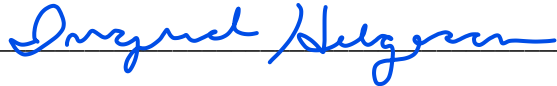
Agreement shall be deemed to create an employment, principal-agent, or partner relationship between the parties. DataHEALTH shall retain sole and absolute discretion in the manner and means of carrying out its activities and responsibilities under this Business Associate Agreement.

11. General Administrative Provisions.

- (a) Any notices required by this Business Associate Agreement will be sent to the latest known address of either party by (i) facsimile, email, registered or certified mail or by private delivery service that provides receipts to the sender and recipient, (ii) personally delivered or (iii) by regular mail. Each party reserves the right to designate an additional address or a separate address for notices to be sent. Notices are deemed given (i) on the date of the facsimile or email transmittal, (ii) the date shown on the registered mail, certified mail or private delivery service receipt, (iii) the date personally delivered, or (iii) two (2) business days after the date of mailing of a notice sent by regular mail.
- (b) Each party agrees to promptly perform any further acts and execute, acknowledge, and deliver any documents which may be reasonably necessary to carry out the provisions of this Business Associate Agreement or effect its purpose.
- (c) In the event that any of the provisions or portions of this Business Associate Agreement are held to be unenforceable or invalid by any court of competent jurisdiction, the validity and enforceability of the remaining provisions or portions will not be affected.
- (d) The waiver by a party of any breach of any term, covenant, or condition in this Business Associate Agreement will not be deemed to be a waiver of any subsequent breach of the same or any other term, covenant, or condition of this Business Associate Agreement. A party's subsequent acceptance of performance by the other party shall not be deemed to be a waiver of any preceding breach of any term, covenant or condition of this Business Associate Agreement other than the failure to perform the particular duties so accepted, regardless of knowledge of such preceding breach at the time of acceptance of the performance.
- (e) This Business Associate Agreement constitutes the entire agreement among the parties with respect to the subject matter of this Business Associate Agreement and supersedes any prior agreements, whether written or oral, pertaining to that subject matter.

CUSTOMER HAS READ, UNDERSTANDS, AND AGREES TO THE TERMS AND CONDITIONS OF THIS BUSINESS ASSOCIATE AGREEMENT WHICH IS ALSO ATTACHED AS AN EXHIBIT TO THE TERMS OF SERVICE AGREEMENT.

DataHEALTH:

By:  _____

Ingrid Helgeson, COO and HIPAA Security Officer

Customer:

Company: _____

By: _____

Name: _____

Title: _____

Date: _____