

# Business Associate Agreement

UPDATED FOR HITECH AND THE HIPAA OMNIBUS RULE

This Business Associate Agreement is entered into by and between OhMD, Inc., a Delaware corporation (“OhMD” or “Business Associate”) and (“Client” or “Covered Entity”), as of the date executed by or on behalf of an authorized representative of Client (“Effective Date”).

WITNESSETH

WHEREAS, the parties have entered into an agreement or agreements (“Agreement(s)”) for the provision of services (which may include transaction services as well as the servicing of hardware and/or software products) (“Services”) that involve the use and/or disclosure of Protected Health Information; and

WHEREAS, OHMD and Client wish to enter into this Business Associate Agreement in order for both parties to establish their respective compliance with the applicable requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and HIPAA Rules.

WHEREAS, the parties wish to enter into this Business Associate Agreement to govern OHMD’s use and disclosure of Protected Health Information and implementation of safeguards for the security of Electronic Protected Health Information under the Agreement(s). OHMD and Client are both committed to complying with (a) HIPAA, (b) the HIPAA Rules, and (c) applicable state law, as these statutes and regulations may be amended from time to time. This Business Associate Agreement sets forth the terms and conditions pursuant to which Protected Health Information will be handled by OhMD as Client’s and Covered Entity’s Business Associate during the term of the Agreement.

OHMD and Client agree as follows:

## 1. DEFINITIONS

1.1. The following capitalized terms used in this Business Associate Agreement shall have the meanings established for purposes of the HIPAA Rules, as amended from time to time: Breach, Data Aggregation, Designated Record Set, Health Care Operations, Individual, Minimum

Necessary, Required by Law, Security Incident, Subcontractor, and Unsecured Protected Health Information.

1.2. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103 and, in reference to a party to this Business Associate Agreement, shall mean OHMD.

1.3. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103 and in reference to a party to this Business Associate Agreement, shall mean Client.

1.4. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Part 160 and Part 164, as amended from time to time.

1.5 “Information Blocking” is a practice described in 45 CFR 171.103 that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information, unless such practice is required by law, or it meets an exception in 45 CFR Part 171.

1.6 “Information System” shall mean an interconnected set of information resources under the same direct management and/or control and that shares common functionality. A system normally includes hardware, software, information, data, applications, communication, and people. For purposes of this Business Associate Agreement, “Information System” shall be limited to that system or systems accessing, storing, or otherwise potentially impacting the privacy or security of Electronic Protected Health Information.

1.7 “Physical Safeguards” shall mean physical measures, policies, and procedures to protect Business Associate electronic Information Systems and related building and equipment, from natural and environmental hazards, and unauthorized intrusion.

1.8. “Protected Health Information” or “PHI” shall mean Protected Health Information, as defined in 45 C.F.R. §, 160.103 and is limited to the Protected Health Information received from, or received or created on behalf of, Covered Entity by Business Associate pursuant to performance of the Services.

1.9 “Security Safeguards” shall mean all of the Administrative, Physical, and Technical Safeguards in an Information System.

1.10 “Technical Safeguards” shall mean the technology and the policy and procedures for its use that protect Electronic Protected Health Information and control access to it.

1.11 “Data Aggregation” shall mean the combining of protected health information from Covered Entity with the protected health information received from other covered entities by Business Associate in its capacity as a business associate of the other covered entities to permit data analyses that relate to the health care operations of Covered Entity and other covered entities.

1.12 “Health care operations” shall have the same meaning as the term “health care operations” at 45 CFR 164.501 including, without limitation, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination.

Terms used, but not otherwise defined, in the Business Associate Agreement shall have the same meaning as those terms as set forth in HIPAA and the HIPAA Rules.

## 2. PERMITTED USES AND DISCLOSURES OF BUSINESS ASSOCIATE

2.1 Services. Business Associate provides services (which may include transaction services, servicing hardware or software products and data analysis) (“Services”) that involve the use and/or disclosure of Protected health Information pursuant to a written Agreement (“Agreement”) with Covered Entity that specify the Services to be provided to Covered Entity. Except as otherwise specified herein, Business Associate may make any and all uses and disclosures of Protected Health Information created or received from or on behalf of Covered Entity necessary to perform its obligations under the Agreement or as may be required by law. Business Associate may perform Data Aggregation for, and related to the Health Care Operations of Covered Entity, including to aggregate Protected Health Information of Covered Entity with Protected Health Information of other covered entities which Business Associate has in its possession through its capacity as a business associate to other covered entities.

2.2 Business Activities of the Business Associate. Business Associate may: (a) consistent with the subject limitations and requirements of the HIPAA Rules, use and disclose the Protected Health Information in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of the Business Associate; (b) de-identify PHI and use or disclose information de-identified in accordance with the HIPAA Rules, and (c) use aggregated data of Covered Entity as combined with the aggregated data of other covered entities that Business Associate has in its possession through its capacity as a business associate to other covered entities to generate de-identified analysis, reports, guidelines, best practices and other materials which do not identify Covered Entity in any manner.

2.3 Disclosures Required By Law. If Business Associate believes it has a legal obligation to disclose any PHI, it will notify Covered Entity as soon as reasonably practical after it learns of such obligation, and in any event at least ten (10) business days prior to the proposed release, as to the legal requirement pursuant to which it believes the Protected Health Information must be released. If Covered Entity objects to the release of such Protected Health Information, Business Associate will allow Covered Entity to exercise any legal rights or remedies Covered Entity might have to object to the release of the Protected Health Information, and Business Associate agrees to provide such assistance to Covered Entity, at Covered Entity's expense, as Covered Entity may reasonably request in connection therewith. Should Covered Entity fail to respond, Business Associate shall be entitled to disclose the Protected Health Information as it deems reasonably necessary to comply with the Law.

### 3. DUTIES AND RESPONSIBILITIES OF THE BUSINESS ASSOCIATE

3.1 Responsibilities of the Business Associate with Respect to Protected Health Information. With regard to its use and/or disclosure of Protected Health Information, Business Associate agrees to:

- (a) use and/or disclose Protected Health Information only as necessary to provide the Services, as permitted or required by this Business Associate Agreement, or as otherwise Required by Law;
- (b) implement and use appropriate safeguards to: (i) prevent use or disclose of Protected Health Information other than as permitted or required by this Business Associate Agreement; and (ii) protect the Electronic Protected Health Information that Business Associate creates,

receives, maintains, or transmits on behalf of the Covered Entity as provided in Subpart C of 45 CFR Part 164;

(c) without unreasonable delay, and in any event on or before 72 hours after its discovered by Business Associate, report to Covered Entity: (i) any use or disclosure of Protected Health Information not provided for by this Business Associate Agreement of which it becomes aware, including Breaches of Unsecured PHI and/or (ii) any Security Incident of which Business Associates becomes aware;

(d) without unreasonable delay, and in any event on or before 72 hours after its Discovery by Business Associate, notify Covered Entity of any Breach or any other incident that involved an unauthorized acquisition, access, use or disclosure of Protected Health Information, even if Business Associate believes the incident will not rise to the level of a Breach. The notification shall include, to the extent possible, and shall be supplemented on an ongoing basis with: (i) the identification of all individuals whose Unsecured Protected Health Information was or is believed to have been involved, (ii) all other information reasonably requested by Covered Entity to enable Covered Entity to perform and document a risk assessment with respect to the incident, and (iii) all other information reasonably necessary to provide notice to individuals, HHS, State officials and/or the media.

Notwithstanding the foregoing, in Covered Entity's sole discretion and in accordance with its directions, Business Associate shall conduct, or pay the costs of conducting, an investigation of any incident required to be reported under this subsection (d) and shall provide, and/or pay the costs of providing the required notices as set forth in this subsection (d);

(e) mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Business Associate Agreement;

(f) require all of its Subcontractors and agents that create, receive, maintain, or transmit Protected Health Information to agree (or has agreed to) in writing, to the same restrictions and conditions on the use and/or disclosure of Protected Health Information that apply to Business Associate; including but not limited to the extent that Business Associate provides Electronic Protected Health Information to a Subcontractor or agent, it shall require the Subcontractor or agent to implement reasonable and appropriate safeguards to protect the Electronic Protected Health

Information consistent with the requirements of this Business Associate Agreement;

(g) make available its internal practices, policies, protocols, books and records related to the use and disclosure of Protected Health Information to the Secretary of HHS for purposes of determining compliance with the HIPAA Rules;

(h) document, and within thirty (30) days after receiving a written request from Covered Entity, make available to Covered Entity information necessary for Covered Entity to make an accounting of disclosures of Protected Health Information about an Individual or, when as directed by Covered Entity, make that information available directly to an individual, all in accordance with the HIPAA Rules and in accordance with the requirements for accounting for disclosures made through an Electronic Health Record;

(i) provide access to Covered Entity after receiving a written request from Covered Entity, to Protected Health Information in a Designated Record Set about an individual, or when and as directed by Covered Entity, provide that access directly to an individual;

(j) notwithstanding subsection (i) above, in the event that Business Associate in connection with the Services uses or maintains an Electronic Health Record of Protected Health Information of or about an individual, then Business Associate shall provide an electronic copy (at the request of Covered Entity, and in the reasonable time and manner requested by Covered Entity) of the Protected Health Information, to covered Entity or, when and as directed by Covered Entity directly to an individual or a third party designated by the individual;

(k) to the extent that the Protected Health Information in Business Associate's possession constitutes a Designated Record Set, make available, within thirty (30) days after a written request by Covered Entity, Protected Health Information for amendment and incorporate any amendments to the Protected Health Information as directed by Covered Entity;

(l) notify Covered Entity in writing within three (3) days after its receipt directly from an individual for any request for an accounting of disclosures, access to, or amendment of Protected Health Information as contemplated in subsections (j)-(k);

(m) use appropriate Administrative, Physical, and Technical safeguards to protect the confidentiality, integrity and availability of any Electronic Protected Health Information in accordance with the HIPAA Rules;

(n) request, use and/or disclose only the Minimum Necessary Protected Health Information to accomplish the purpose of a request, use or disclosure permitted under the HIPAA Rules;

(o) not directly or indirectly receive remuneration in exchange for any Protected Health Information;

(p) not make or cause to be made any communication about a product or service that is prohibited by the HIPAA Rules; and

(q) not make or cause to be made any written fundraising communication that is prohibited by the HIPAA Rules.

### 3.2 Responsibilities of the Covered Entity with Respect to Protected Health Information.

(a) With regard to the use and/or disclosure of Protected Health Information by the Business Associate, the Covered Entity agrees: (i) to obtain any consent, authorization or permission that may be required by the HIPAA Rules or any other applicable federal, state or local laws and/or regulations prior to disclosing to or furnishing Business Associate with the Protected Health Information pertaining to an individual; and (ii) that it will not furnish Business Associate Protected Health Information that is subject to any arrangements permitted or required of the Covered Entity, unless it has provided Business Associate with written notification of any such arrangement, including but not limited to, arrangements agreed to by Covered Entity that may impact in any manner the use and/or disclosure of Protected Health Information by the Business Associate under this Business Associate Agreement and the Agreement.

(b) Covered Entity represents and warrants that its notice of privacy practices permits Covered Entity to use and disclose Protected Health Information in the manner that Business Associate is authorized to use and disclose Protected Health Information under this Business Associate Agreement.

(c) Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices in accordance with 45 C.F.R. § 164.520 to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(d) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an individual to use or disclose Protected Health Information to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(e) Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy and Security Rules if done by Covered Entity.

#### 4. TERM AND TERMINATION

4.1 Term. The Term of this Business Associate Agreement shall commence as of the Effective Date of the Agreement and shall terminate either (a) as provided by Section 4.2 below or (b) when all of the Protected Health Information or Electronic Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, or otherwise in Business Associate's possession, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information in accordance with the termination provisions in this Section.

4.2 Termination for Cause. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity (i) may provide a reasonable time for Business Associate to cure the breach provided that Covered Entity may immediately terminate the Business Associate Agreement that requires the use of Protected Health Information or Electronic Protected Health Information if Business Associate does not cure the breach or end the violation within the time frame specified by Covered Entity; (ii) immediately terminate the Agreement that requires the use of Protected Health Information if Business Associate has breached a material term of this Business Associate Agreement and Covered Entity determines in its sole reasonable discretion that a cure is not possible; or (iii) if neither termination nor cure is feasible, may report the violation to the Secretary.



### 4.3 Effect of Termination

4.3.1 Except as provided in paragraph 4.3.2 of this Section, upon termination of this Business Associate Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information and Electronic Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, or otherwise in Business Associate's possession. Business Associate shall retain no copies of the Protected Health Information or Electronic Protected Health Information in any form.

4.3.2 In the event that Business Associate determines that returning or destroying the Protected Health Information or Electronic Protected Health Information is infeasible, Business Associate agrees to extend the protections of this Business Associate Agreement to such Protected Health Information and limit any further uses and disclosures of such Protected Health Information to only those purposes that make the return or destruction infeasible.

## 5. MISCELLANEOUS

5.1 Regulatory References. A reference in this Business Associate Agreement to a section in the HIPAA Rules means the section as in effect or as amended, and for which compliance is required.

5.2 Information Blocking Rules. Business Associate will support the Covered Entity's timely access, exchange, and use of electronic health information to comply with 45 CFR Part 171, the Information Blocking Rules promulgated under the 21<sup>st</sup> Century Cures Act (2016).

5.3 Amendment. This Business Associate Agreement may only be modified, or any rights under it waived, by a written agreement executed by both parties. The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for the parties to comply with the requirements of HIPAA or other state or federal law and any current or future regulations promulgated thereunder.

5.4 Interpretation. Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Rules and any current or future regulations promulgated thereunder.

5.5 Waiver. Any failure of a party to exercise or enforce any of its rights under this Business Associate Agreement will not act as a waiver of such rights.

5.6 Binding Effect. The Business Associate Agreement shall be binding upon, and shall inure to the benefit of, the parties and their respective successors and permitted assigns.

5.7 No Third Party Beneficiaries. Nothing expressed or implied in this Business Associate Agreement is intended or shall be deemed to confer upon any person other than Covered Entity and Business Associate, and their respective successors and assigns, any rights, obligations, remedies or liabilities.

5.8 Severability. If any provision of this Business Associate Agreement is held by a court of competent jurisdiction to be illegal, invalid or unenforceable under present or future laws effective during the term of this Business Associate Agreement, the legality, validity and enforceability of the remaining provisions shall not be affected thereby.

5.9 Counterparts. This Business Associate Agreement may be executed in counterparts, each of which shall be deemed an original but all of which shall constitute on and the same instrument.

5.10 No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor anything herein shall confer, upon any person other than the parties hereto any rights, remedies, obligations, or liabilities whatsoever.

5.11 Notices. Any notices to be given hereunder shall be made via email to [privacy@ohmd.com](mailto:privacy@ohmd.com)