

## BUSINESS ASSOCIATE AGREEMENT

This **BUSINESS ASSOCIATE AGREEMENT** (this “**BA Agreement**”) is made by and between DermDash Inc., a California Corporation (“**Company**”), and the Physician / Medical Practice registering today (“**Covered Entity**”) and is effective as of the electronic stamped date on the submitted application (“**Effective Date**”). Capitalized terms used in this BA Agreement without definition shall have the respective meanings assigned to such terms in the Administrative Simplification section of the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act and their implementing regulations as amended from time to time (collectively, “**HIPAA**”).

### RECITALS

**WHEREAS**, Covered Entity and Company are parties to certain agreement(s) setting forth certain services that require Company to have access to Protected Health Information (collectively, the “License Agreement”);

**WHEREAS**, Company and Covered Entity have previously entered into a Business Associate Agreement in connection with the License Agreement (the “**Original BA**”); and

**WHEREAS**, Company and Covered Entity desire to replace the Original BA with this BA Agreement.

**NOW THEREFORE**, in consideration of the mutual premises and covenants contained herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Covered Entity and Company agree as follows:

### AGREEMENT

#### I. GENERAL PROVISIONS.

**Section 1.1** **Effect.** The provisions of this BA Agreement shall control with respect to Protected Health Information that Company receives from or on behalf of Covered Entity (“**PHI**”), and the terms and provisions of this BA Agreement hereby supersede and replace the Original BA in its entirety.

**Section 1.2** **No Third Party Beneficiaries.** The parties have not created and do not intend to create by this BA Agreement any third party rights, including, but not limited to, third party rights for Covered Entity’s patients.

**Section 1.3** **HIPAA Amendments.** The parties acknowledge and agree that the Health Information Technology for Economic and Clinical Health Act and its implementing regulations impose requirements with respect to privacy, security and breach notification applicable to Business Associates (collectively, the “**HITECH BA Provisions**”). The HITECH BA Provisions and any other future amendments to HIPAA affecting Business Associate

Agreements are hereby incorporated by reference into this BA Agreement as if set forth in this BA Agreement in their entirety, effective on the later of the effective date of this BA Agreement or such subsequent date as may be specified by HIPAA.

Agreements are hereby incorporated by reference into this BA Agreement as if set forth in this BA Agreement in their entirety, effective on the later of the effective date of this BA Agreement or such subsequent date as may be specified by HIPAA.

**Section 1.4 Regulatory References.** A reference in this BA Agreement to a section in HIPAA means the section as it may be amended from time-to-time.

## **II. COMPANY'S OBLIGATIONS.**

**Section 2.1 Use and Disclosure of PHI.** Company may use and disclose PHI as permitted or required under the License Agreement, this BA Agreement and as Required by Law, but shall not otherwise use or disclose any PHI. Company shall not use or disclose PHI received from Covered Entity in any manner that would constitute a violation of HIPAA if so used or disclosed by Covered Entity (except as set forth in Sections 2.1(a), (b) and (c) of this BA Agreement). To the extent Company carries out any of Covered Entity's obligations under the HIPAA Privacy Rule, Company shall comply with the requirements of the HIPAA Privacy Rule that apply to Covered Entity in the performance of such obligations. Without limiting the generality of the foregoing, Company is permitted to use or disclose PHI as set forth below:

(a) Company may use PHI internally for its proper management and administrative services or to carry out its legal responsibilities;

(b) Company may disclose PHI to a third party for Company's proper management and administration, provided that the disclosure is Required by Law or Company obtains reasonable assurances from the third party to whom the PHI is to be disclosed that the third party will (1) protect the confidentiality of the PHI, (2) only use or further disclose the PHI as Required by Law or for the purpose for which the PHI was disclosed to the third party and (3) notify Company of any instances of which the person is aware in which the confidentiality of the PHI has been breached;

(c) Company may use PHI to provide Data Aggregation services as defined by HIPAA; and

(d) Company may use PHI to create de-identified health information in accordance with the HIPAA de-identification requirements. Without limiting Company's rights under the License Agreement, Company may disclose, use and/or exploit deidentified health information for any purposes not prohibited by law. For the avoidance of doubt, the second sentence of this Section 2.1(d) shall survive the expiration or earlier termination of this BA Agreement.

**Section 2.2 Safeguards.** Company shall use reasonable and appropriate safeguards to

prevent the use or disclosure of PHI, except as otherwise permitted or required by this BA Agreement. In addition, Company shall implement Administrative Safeguards, Physical Safeguards and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of PHI transmitted or maintained in Electronic Media (“**EPHI**”) that it creates, receives, maintains or transmits on behalf of Covered Entity. Company shall comply with the HIPAA Security Rule with respect to EPHI.

**Section 2.3 Minimum Necessary Standard.** To the extent required by the “minimum necessary” requirements of HIPAA, Company shall only request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure.

**Section 2.4 Mitigation.** Company shall take reasonable steps to mitigate, to the extent practicable, any harmful effect (that is known to Company) of a use or disclosure of PHI by Company in violation of this BA Agreement.

**Section 2.5 Subcontractors.** Company shall enter into a written agreement meeting the requirements of 45 C.F.R. §§ 164.504(e) and 164.314(a)(2) with each Subcontractor (including, without limitation, a Subcontractor that is an agent under applicable law) that creates, receives, maintains or transmits PHI on behalf of Company. Company shall ensure that the written agreement with each Subcontractor obligates the Subcontractor to comply with restrictions and conditions that are at least as restrictive as the restrictions and conditions that apply to Company under this BA Agreement.

**Section 2.6 Reporting Requirements.**

(a) If Company becomes aware of a use or disclosure of PHI in violation of this BA Agreement by Company or by a third party to which Company disclosed PHI, Company shall report any such use or disclosure to Covered Entity without unreasonable delay.

(b) Company shall report any Security Incident involving EPHI of which it becomes aware in the following manner: (a) any actual, successful Security Incident will be reported to Covered Entity in writing without unreasonable delay, and (b) any attempted, unsuccessful Security Incident of which Company becomes aware will be reported to Covered Entity orally or in writing on a reasonable basis, as requested by Covered Entity. If the HIPAA security regulations are amended to remove the requirement to report unsuccessful attempts at unauthorized access, the requirement hereunder to report such unsuccessful attempts will no longer apply as of the effective date of the amendment.

(c) Company shall, following the discovery of a Breach of Unsecured PHI, notify the Covered Entity of such Breach in accordance with 45 C.F.R. § 164.410 without unreasonable delay and in no case later sixty (60) days after discovery of the Breach.

**Section 2.7 Access to Information.** Company shall make available PHI in EMA (as defined below) to Covered Entity in accordance with the License Agreement for so long as Company maintains the PHI in a Designated Record Set. If Company receives a request for access to PHI directly from an Individual, Company shall forward such request to Covered Entity within ten (10) business days. Covered Entity shall have the sole responsibility for determining whether to approve a request for access to PHI and to provide such access to the Individual.

**Section 2.8 Availability of PHI for Amendment.** Company shall provide PHI in EMA to Covered Entity for amendment, and incorporate any such amendments in the PHI (for so long as Company maintains such information in the Designated Record Set), in accordance with the License Agreement and as required by 45 C.F.R. § 164.526. If Company receives a request for amendment to PHI directly from an Individual, Company shall forward such request to Covered Entity within ten (10) business days. Covered Entity shall have the sole responsibility for determining whether to approve an amendment to PHI and to make such amendment.

**Section 2.9 Accounting of Disclosures.** Within thirty (30) business days of written notice by Covered Entity to Company that it has received a request for an accounting of disclosures of PHI (other than disclosures to which an exception to the accounting requirement applies), Company shall make available to Covered Entity such information as is in Company's possession and is required for Covered Entity to make the accounting required by 45 C.F.R. § 164.528. Covered Entity shall have the sole responsibility for providing an accounting to the Individual.

**Section 2.10 Availability of Books and Records.** Following reasonable advance written notice, Company shall make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Company on behalf of, Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with HIPAA.

### **III. TERMINATION OF THE AGREEMENT.**

**Section 3.1 Term.** The term of this BA Agreement shall commence on the Effective Date and shall continue for so long as Company maintains any PHI.

**Section 3.2 Termination Upon Breach of Provisions Applicable to PHI.** Any other provision of the License Agreement notwithstanding, the License Agreement may be terminated by either party (the "**Non-Breaching Party**") upon thirty (30) days written notice to the other party (the "**Breaching Party**") in the event that the Breaching Party materially breaches this BA Agreement in any material respect and such breach is not cured within such thirty (30) day period.

**Section 3.3 Return or Destruction of PHI upon Termination.** Upon termination of this BA Agreement, Company shall return or destroy all PHI received from Covered Entity or

created or received by Company on behalf of Covered Entity and which Company still maintains as PHI. Notwithstanding the foregoing, to the extent that Company determines that it is not feasible to return or destroy such PHI, this BA Agreement (including, without limitation, Section 2.1(d)) shall survive termination of the License Agreement and such PHI shall be used or disclosed solely for such purpose or purposes which prevented the return or destruction of such PHI.

#### **IV. OBLIGATIONS OF COVERED ENTITY.**

**Section 4.1 Permissible Requests.** Covered Entity shall not request Company to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

**Section 4.2 . Minimum Necessary PHI.** When Covered Entity discloses PHI to Company, Covered Entity shall provide the minimum amount of PHI necessary for the accomplishment of Covered Entity's purpose.

**Section 4.3 Appropriate Use of PHI.** Covered Entity and its employees, representatives, consultants, contractors and agents shall not submit any Protected Health Information to Company (A) outside of Company's proprietary web-based software marketed under the name Electronic Medical Assistant or EMA ("**EMA**"), including but not limited to submissions to any online forum made available by Company to its customers, email transmissions, and submissions through any support website, portal, or online help desk or similar service made available by Company outside of EMA; or (B) directly to any third party involved in the provision of an online forum, email, support website, online help desk or other service described in (A), above.

**Section 4.4 Notice of Privacy Practices.** Except as Required By Law, with Company's consent or as set forth in the License Agreement or this BA Agreement, Covered Entity shall not include any limitation in the Covered Entity's notice of privacy practices that limits Company's use or disclosure of PHI under the License Agreement.

**Section 4.5 Permissions; Restrictions.** Covered Entity warrants that it has obtained and will obtain any consent, authorization and/or other legal permission required under HIPAA and other applicable law for the disclosure of PHI to Company. Covered Entity shall notify Company 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 Company's use or disclosure of PHI. Covered Entity shall not agree to any restriction on the use or disclosure of PHI under 45 CFR § 164.522 that restricts Company's use or disclosure of PHI under this Agreement unless such restriction is Required By Law or Company grants its written consent, which consent shall not be unreasonably withheld.

#### **V. MISCELLANEOUS.**

**Section 5.1 Amendments; Waiver.** This BA Agreement may not be modified, nor

shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

**Section 5.2 Notices.** Any notices to be given hereunder to a party shall be made via hand delivery, U.S.P.S. Certified Mail Return Receipt Requested, or nationally recognized express courier with proof of delivery, to such party's address as set in the License Agreement and shall be effective upon actual delivery.

**Section 5.3 Enforcement Costs.** If any legal action or other proceeding is brought for the enforcement or interpretation of this BA Agreement, or because of an alleged dispute, breach, default or misrepresentation in connection with any provision of this BA Agreement, the substantially prevailing party shall be entitled to recover reasonable attorneys' fees, court costs and all expenses incurred in that action or proceeding and at all levels of trial and appeal, in addition to any other relief to which such party may be entitled.

**Section 5.4 Limitation of Liability.** IN NO EVENT SHALL COMPANY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS BA AGREEMENT, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED THE AMOUNTS ACTUALLY PAID BY AND DUE FROM COVERED ENTITY UNDER THE LICENSE AGREEMENT DURING THE ONE (1) YEAR PERIOD IMMEDIATELY PRECEDING THE DATE THE CAUSE OF ACTION AROSE.

**Section 5.5 Exclusion of Consequential Damages.** IN NO EVENT SHALL COMPANY HAVE ANY LIABILITY TO COVERED ENTITY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY WHETHER OR NOT COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR THE LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES OR JURISDICTIONS, COMPANY'S LIABILITY SHALL BE LIMITED TO THE MAXIMUM EXTENT PERMITTED BY LAW.

**Section 5.6 Counterparts; Facsimiles.** This BA Agreement may be executed in any number of counterparts, which may be delivered by facsimile or other electronic transmission, including email, each of which shall be deemed an original.

**[Remainder of page left intentionally blank]**

**IN WITNESS WHEREOF**, the parties hereto have duly executed this BA Agreement.

**DermDash Inc.**

By: Ben Behnam

Name: Ben Behnam MD

Title: CEO & President

Date: 03/24/2016

**Covered Entity**

BY CHECKING "ACCEPT" AND SIGNING THE ELECTRONIC SIGNATURE, YOU AGREE THAT YOU ARE THE LEGAL REPRESENTATIVE FOR THE PHYSICIAN AND MEDICAL PRACTICE AND THAT YOU HAVE READ AND AGREE TO THE ABOVE BA AGREEMENT. THE AGREEMENT IS BINDING AS OF TODAY'S DATE, WHICH IS ELECTRONICALLY TIME STAMPED WHEN THE APPLICATION IS SUBMITTED.