

## Business Associate Agreement

This Business Associate Agreement (this “BAA”), is entered into, by and between Optos, Inc. (the “Business Associate”) and the Customer (the “Covered Entity”) (each a “Party” and collectively the “Parties”). The Parties hereby agree as follows:

### 1. Definitions.

Capitalized terms used herein shall have the meanings set out against them below or as established for purposes of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended and supplemented by ARRA and its implementing regulations, as each is amended from time to time (collectively, “HIPAA”).

“ARRA” means Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 17921–17954, and all associated existing and future implementing regulations, when and as each is effective.

“Breach” means the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI as defined, and subject to the exclusions set forth, in 45 C.F.R. § 164.402.

“ePHI” means PHI that is transmitted or maintained in Electronic Media.

“PHI” or “Protected Health Information” shall have the meaning set forth in 45 C.F.R. § 160.103, and is limited to the Protected Health Information received from, or received, maintained, created or transmitted on behalf of, Covered Entity by Business Associate in performance of the Services.

“Privacy Rule” means the regulations, as amended from time to time, codified at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

“Security Rule” means the regulations, as amended from time to time, codified at 45 C.F.R. Part 160 and Part 164, Subparts A and C.

“Services” means, to the extent and only to the extent they involve the creation, receipt, maintenance, transmission, use or disclosure of PHI, the services provided by Business Associate to Covered Entity as set forth in the product order form, including those set forth in Section 4 of this BAA, as amended by written agreement of the Parties from time to time.

### 2. Business Associate Obligations.

Business Associate agrees to:

- (a) not use and/or further disclose PHI except as necessary to provide the Services, as permitted or required by this BAA, and in compliance with each applicable requirement of 45 C.F.R. § 164.504(e), or as otherwise Required by Law;
- (b) to the extent Business Associate is to carry out Covered Entity’s obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of those obligations;
- (c) without unreasonable delay, report to Covered Entity:
  - (i) any use or disclosure of PHI not provided for by this BAA of which it becomes aware in accordance with 45 C.F.R. § 164.504(e)(2)(ii)(C), and/or
  - (ii) any Security Incident of which Business Associate becomes aware in accordance with 45 C.F.R. § 164.314(a)(2)(i)(C);
- (d) in the event of a Breach, and without unreasonable delay, and in any event no later than sixty (60) calendar days after Discovery, Business Associate shall provide Covered Entity with written notification in accordance with 45 C.F.R. § 164.410;

(e) implement and use appropriate administrative, physical and technical safeguards with respect to PHI, and comply with applicable Security Rule requirements with respect to ePHI, to prevent use or disclosure of PHI other than as provided for by this BAA;

(f) in accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 164.308(b)(2), ensure that any subcontractors of Business Associate that create, receive, maintain or transmit PHI on behalf of Business Associate agree, in writing, to restrictions and conditions on the use and/or disclosure of PHI that are no less restrictive than those that apply to Business Associate with respect to that PHI, including complying with the applicable Security Rule requirements with respect to ePHI;

(g) make available its internal practices, books and records relating to the use and disclosure of PHI to the Secretary during normal business hours for purposes of determining the Parties' compliance with the Privacy Rule;

(h) to the extent that PHI in Business Associate's possession constitutes a Designated Record Set, Business Associate shall:

(i) provide access, within twenty (20) days after receiving a written request from Covered Entity, to the PHI about an Individual, to Covered Entity, sufficient to allow Covered Entity to comply with the requirements of 45 C.F.R. § 164.524, including providing or sending a copy to a designated third party and providing or sending a copy in electronic format in accordance with 45 C.F.R. § 164.524; and

(ii) make available, within thirty (30) days after a written request by Covered Entity, the PHI for amendment and incorporate any amendments to the PHI as requested by Covered Entity, all in accordance with 45 C.F.R. § 164.526; and

(i) 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 PHI about an Individual, in accordance with 45 C.F.R. § 164.528

and, as of the later of the date compliance is required by final regulations or the Effective Date, 42 U.S.C. § 17935(c).

### **3. Covered Entity Obligations.**

In addition to other obligations set forth in this BAA, Covered Entity:

(a) shall identify the records it furnishes to Business Associate that is PHI;

(b) shall provide to Business Associate only the minimum PHI necessary to accomplish the Services;

(c) agrees not to provide Business Associate any PHI that is subject to any restriction on the use or disclosure of PHI pursuant to 45 C.F.R. § 164.522(a) or any additional limitations imposed on Covered Entity because of revisions to its notice of privacy practices in accordance with 45 C.F.R. § 164.520;

(d) shall be responsible for using administrative, physical and technical safeguards at all times to maintain and ensure the confidentiality, privacy and security of PHI transmitted to Business Associate in accordance with HIPAA;

(e) shall obtain any consent or authorization that may be required by applicable federal or state laws and regulations prior to furnishing Business Associate the PHI for use and disclosure in accordance with this BAA; and

(f) comply with its obligations under HIPAA for making all required notices upon the discovery of a Breach of Unsecured PHI, in accordance with federal breach regulations, as amended from time to time, issued pursuant to HIPAA and codified at 45 C.F.R. Part 164, Subpart D.

### **4. Additional Uses and Disclosures.**

Unless otherwise provided in this BAA, in addition to any other uses and/or disclosures permitted or required by this BAA, Business Associate may:

(a) use and disclose PHI necessary to provide the Services to Covered Entity;

(b) use and disclose PHI, if necessary, for proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that the disclosures are Required by Law or any third party to which Business Associate discloses PHI for those purposes provides written assurances in advance that:

(i) the information will be held confidentially and used or further disclosed only for the purpose for which it was disclosed to the third party or as Required by Law; and

(ii) the third party promptly will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the information has been breached;

(c) De-identify any and all PHI received or created by Business Associate under this BAA, which De-identified information shall not be subject to this BAA; and

(d) provide Data Aggregation services relating to the Health Care Operations of Covered Entity in accordance with the Privacy Rule.

## 5. Term and Termination.

(a) The term of this BAA shall commence as of the signing of the Product Order From , and, unless terminated as set forth herein, shall terminate when Business Associate is no longer providing any services for Covered Entity.

(b) If either Party knows of a pattern of activity or practice of the other Party that constitutes a material breach or violation of this BAA, then the non-breaching Party shall provide written notice of the breach or violation to the other Party that specifies the nature of the breach or violation. The breaching Party must cure the breach or end the violation on or before thirty (30) days after receipt of the written notice. In the absence of a cure reasonably satisfactory to the non-breaching Party within the specified timeframe, or in the event the

breach is reasonably incapable of cure, then the non-breaching Party may terminate this BAA.

(c) Within sixty (60) days after the expiration or termination of this BAA, Business Associate shall return or destroy all PHI, if feasible to do so, including all PHI in possession of Business Associate's subcontractors. In the event that Business Associate determines that return or destruction of the PHI is not feasible, Business Associate may retain the PHI subject to this Section 5(c). Under any circumstances, Business Associate shall extend any and all protections, limitations and restrictions contained in this BAA to Business Associate's use and/or disclosure of any PHI retained after the expiration or termination of this BAA, and shall limit any further uses and/or disclosures solely to the purposes that make return or destruction of the PHI infeasible.

## 6. Construction of Terms.

The terms of this BAA to the extent they are unclear shall be construed to allow for compliance by Covered Entity and Business Associate with HIPAA.

## 7. Survival.

Sections 5(c) and 6-14 shall survive the expiration or termination for any reason of this BAA.

## 8. Counterparts.

This BAA may be executed in counterparts, each of which will constitute an original and all of which will be one and the same document.

## 9. Governing Law.

This BAA shall be governed by and construed in accordance with the laws of the State of Delaware without regard to its provisions regarding conflict of laws.

**10. No Agency or Joint Venture Relationship.**

Nothing contained herein shall be deemed to create any association, partnership, joint venture or relationship of principal, agent, master or servant between Business Associate and Covered Entity, or to provide Business Associate or Covered Entity with the right, power or authority to incur any obligation or make any representations, warranties or guarantees on behalf of any other Party.

**11. Third Parties.**

Any person who is not a Party to this BAA shall not have any rights under or in connection with it.

**12. Cooperation.**

Each Party shall cooperate in good faith in all respects with the other Party in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry.

**13. Notices.**

All notices hereunder shall be in writing and shall be deemed to have been given when delivered in hand, when sent by registered or certified mail, return receipt requested, or when sent by commercial overnight courier (such as Federal Express), to the address defined by the contract number. Either Party may designate a different address by giving notice in the manner herein provided.

**14. Renegotiation and Amendment.**

The Parties agree to negotiate in good faith any modification to this BAA that may be necessary or required to ensure consistency with amendments to and changes in applicable federal and state laws and regulations, including but not limited to HIPAA.