



## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“Agreement”) is entered into by and between \_\_\_\_\_ (“Customer”) and Insight Optics, Inc. (“Business Associate”) and shall be effective as of \_\_\_\_\_.

### RECITALS

WHEREAS, Business Associate may create, receive, maintain, or transmit protected health information on behalf of Customer in conjunction with the services described in the Agreement;

WHEREAS, such protected health information may be used or disclosed only in accordance with the Privacy Rule issued by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”);

WHEREAS, Business Associate must safeguard any electronic protected health information that it creates, receives, maintains, or transmits on behalf of Customer as required by the Security Rule issued by the U.S. Department of Health and Human Services under HIPAA; and

WHEREAS, Subtitle D of the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) provisions in the American Recovery and Reinvestment Act of 2009 (“ARRA”) amended HIPAA and its implementing regulations.

NOW THEREFORE, the parties agree as follows:

### 1. DEFINITIONS

Unless otherwise provided for in this Agreement, terms used in this Agreement shall have the same meanings as set forth in HIPAA, ARRA, the Privacy Rule and the Security Rule.

“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 any and all references in this Agreement to sections of ARRA shall be deemed to include all associated existing and future implementing regulations, when and as each is effective.

“Availability” means the property that data or information is accessible and useable upon demand by an authorized person.

“Breach” shall mean 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 exceptions set forth, in 45 C.F.R. 164.402.

“Business Associate” means an entity or a person that performs a function on behalf of, or provides a service to, Customer that involves the creation, receipt, use or disclosure of PHI.

“Compliance Date” shall mean, in each case, the date by which compliance is required under the referenced provision of ARRA and/or its implementing regulations, as applicable; provided that, in any case for which that date occurs prior to the effective date of this Agreement, the Compliance Date shall mean the effective date of this Agreement.

“Confidentiality” means the property that data or information is not made available or disclosed to unauthorized persons or processes.

“Electronic Protected Health Information” (“Electronic PHI”) means Protected Health Information that is transmitted by, or maintained in, electronic media.

“Integrity” means the property that data or information have not been altered or destroyed in an unauthorized manner.

“Protected Health Information” (“PHI”) means individually identifiable information, transmitted or maintained in any form or medium, relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual, as more fully defined in 45 CFR § 160.103, and any amendments thereto.

“Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information, set forth at 45 CFR Parts 160 and 164.

“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 Rule” means the Security Standards for the Protection of Electronic Protected Health Information, set forth at 45 CFR Parts 160 and 164.

“Services” shall mean, to the extent and only to the extent they involve the creation, use or disclosure of PHI, the services provided by Business Associate to Customer under the Agreement, including those set forth in this Agreement, as amended by written agreement of the parties from time to time.

“Unsecured PHI” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services (HHS) in guidance issued pursuant to ARRA.

## **2. GENERAL PROVISIONS**

2.1 Effect. This Agreement supersedes any agreements between the parties involving the disclosure of PHI by Customer to Business Associate. To the extent any conflict or inconsistency between this Agreement and the terms and conditions of any agreement exists, the terms of this Agreement shall prevail.

2.2 Amendment. The parties agree to amend this Agreement as necessary to comply with the Privacy Rule, the Security Rule, and such other regulations promulgated by the Secretary of Health and Human Services pursuant to HIPAA.

## **3. SCOPE OF USE AND DISCLOSURE**

3.1 Business Associate may use or disclose PHI as required to provide Services and satisfy its obligations under the Agreement, if such use or disclosure of PHI would not violate the Privacy Rule. Unless otherwise limited herein, Business Associate may use or disclose PHI:

- a. for Business Associate’s proper management and administrative services;
- b. to carry out the legal responsibilities of Business Associate; and
- c. to provide data aggregation services relating to the health care operations of Customer if required under the Agreement

- d. when de-identified in accordance with 45 CFR 164.514(b)(2)(i) as de-identified information does not constitute Protected Health Information and is not subject to the terms of this agreement.

3.2 Business Associate shall not request, use or release more than the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure and shall comply with 42 U.S.C. § 17935(b) as of its Compliance Date. Business Associate hereby acknowledges that all PHI created or received from, or on behalf of, Customer is the sole property of Customer.

3.3 Business Associate or its agents or subcontractors shall not perform any work outside the United States of America that involves access to, or the disclosure of, PHI without the prior written consent of Customer.

3.4 As of the Compliance Date, Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI as prohibited by 42 U.S.C. § 17935(d) as of its Compliance Date.

3.5 As of the Compliance Date, Business Associate shall not make or cause to be made any communication about a product or service that is prohibited by 42 U.S.C. § 17936(a) as of its Compliance Date.

3.6 As of the Compliance Date, Business Associate shall not make or cause to be made any written fundraising communication that is prohibited by 42 U.S.C. § 17936(b) as of its Compliance Date.

#### **4. OBLIGATIONS OF BUSINESS ASSOCIATE**

Business Associate shall:

4.1 Use or disclose PHI only as permitted or required by this Agreement or as required by law.

4.2 Establish and use appropriate safeguards to prevent unauthorized use or disclosure of PHI.

4.3 Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of Customer. Business Associate shall, as of the Compliance Date of 42 U.S.C. § 17931, comply with the Security Rule requirements set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316.

4.4 Promptly report to Customer any unauthorized use or disclosure of PHI, or security incident, within no more than three (3) days after Business Associate becomes aware of the unauthorized use or disclosure of PHI or Security Incident. Business Associate shall take all reasonable steps to mitigate any harmful effects of such breach or security incident. Business Associate shall indemnify Customer against any losses, damages, expenses or other liabilities including reasonable attorney's fees incurred as a result of Business Associate's or its agent's or subcontractor's unauthorized use or disclosure of PHI or Breach of Unsecured PHI including, but not limited to, the costs of notifying individuals affected by a Breach of Unsecured PHI.

4.5 Business Associate shall, following discovery of a Breach of Unsecured PHI that is caused by Business Associate or its agents or subcontractors, notify Customer of such Breach, without unreasonable delay, and in no event more than thirty (30) days after the discovery of the Breach. The notification by the Business Associate to Customer shall include: (1) the identification of each individual whose Unsecured PHI was accessed, acquired, used or disclosed during the Breach; and (2) any other available information that Customer is required to include in its notification to individuals affected by the Breach including, but not limited to, the following:

- a. a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach;
- b. a description of the types of Unsecured PHI that were involved in the Breach;
- c. a brief description of what the Business Associate is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches.

4.6 Ensure that all of its subcontractors and agents are bound by the same restrictions and obligations contained herein, whenever PHI is made accessible to such subcontractors or agents.

4.7 Within ten (10) days of receiving a request, make all PHI and related information in its possession available as follows:

- a. To the individual or Customer to the extent necessary to permit Customer to respond to an individual's request for access to their PHI for inspection and copying in accordance with 45 CFR § 164.524, to the extent the PHI is maintained in a Designated Record Set;
- b. To the individual or Customer to the extent necessary to permit Customer to make an accounting of disclosures of PHI about the individual, in accordance with 45 CFR § 164.528. At a minimum, Business Associate shall provide Customer with the following information: (i) the date of the disclosure, (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure;
- c. In the event that Business Associate in connection with the Services uses or maintains an Electronic Health Record of PHI of or about an individual, then Business Associate shall provide an accounting of disclosures of PHI, within ten (10) days, to Customer, or when and as directed by Customer, directly to an individual in accordance with the requirements for accounting for disclosures made through an Electronic Health Record in 42 U.S.C. 17935(c), as of its Compliance Date.

4.8 Within fifteen (15) days of receiving a request from Customer, incorporate any amendment or correction to the PHI in accordance with the Privacy Rule, to the extent the PHI is maintained in a Designated Record Set.

4.9 Make its internal practices, books and records relating to the use or disclosure of PHI received from or on behalf of Customer available to Customer or the U. S. Secretary of Health and Human Services for purposes of determining compliance with the Privacy Rule.

4.10 Upon termination of the Agreement, Business Associate shall, at the option of Customer, return or destroy all PHI created or received from, or on behalf of, Customer. Business Associate shall not retain any copies of PHI except as required by law. If PHI is destroyed, Business Associate agrees to provide Customer with certification of such destruction. If return or destruction of all PHI, and all copies of PHI, is not feasible, Business Associate shall extend the protections of this Agreement to such information for as long as it is maintained. Termination of the Agreement attached hereto shall not affect any of its provisions that, by wording or nature, are intended to remain effective and to continue in operation.

4.11 Standard Transactions. To the extent Business Associate conducts Standard Transaction(s) on behalf of Customer, Business Associate shall comply with the HIPAA Regulations, "Administrative Requirements," 45 C.F.R. § 162.100 et seq., by the applicable compliance date(s) and shall not: (a) Change the definition, data condition or use of a data element or segment in a standard; (b) Add any data elements or segments to the maximum defined data set; (c) Use any code or data elements that are either marked "not used" in the standard's implementation specification or are not in the standard's implementation specification(s); or (d) Change the meaning or intent of the standard's implementation specifications.

4.12 Restriction of PHI for Self-Pay. Customer shall notify Business Associate within five (5) days of any restriction to the use or disclosure of PHI requested by an Individual in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

## **5. INDEMNIFICATION**

Each party will indemnify and defend the other party from and against any and all claims, losses, damages, expenses or other liabilities, including reasonable attorney's fees, incurred as a result of any breach by such party of any representation, warranty, covenant, agreement or other obligation contained herein by such party, its employees, agents, subcontractors or other representatives.

**6. TERMINATION OF AGREEMENT**

Notwithstanding any other provision of this Agreement or the Agreement, Customer may terminate this Agreement and the Agreement upon five (5) days written notice to Business Associate if Customer determines, in its sole discretion, that Business Associate has violated a material term of this Agreement and such breach is not cured within such five (5) day period.

**7. MISCELLANEOUS**

7.1 Regulatory References. A reference in this Agreement to a section in HIPAA means the section as in effect or as amended.

7.3 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with HIPAA rules and any other applicable law.

7.4 No Third Party Beneficiaries. The terms and conditions of this Agreement, express or implied, exist only for the benefit of the parties to this Agreement and their respective successors and assigns. No other person or entity will be deemed to be a third party beneficiary of this Agreement.

7.5 Notices. Any notices to be given hereunder shall be made via U.S. mail, express courier or hand delivery to the other parties address given below as follows:

If to Customer:

If to Business Associates:  
Insight Optics, Inc.  
967 Wolfe Ln NW  
Atlanta, GA 30318  
Telephone: 954.806.3673

**INTENDING TO BE LEGALLY BOUND**, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

**BUSINESS ASSOCIATE**

\_\_\_\_\_

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_