

OMIC BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT is executed this 17th day of February, 2010, by Ophthalmic Mutual Insurance Company, a risk retention group (OMIC).

Recitals

OMIC and the insured have an insurer/insured relationship by virtue of a professional and limited office premises liability insurance policy issued by OMIC to the insured, hereinafter, "Insurance Policy." OMIC may need to use and/or disclose Protected Health Information ("PHI") in its performance of services under the Insurance Policy. OMIC intends to protect the privacy and provide for the security of PHI disclosed to it in compliance with the HIPAA Rules and HITECH Standards. Under HIPAA, the insured is a "Covered Entity" and OMIC is a "Business Associate" of the insured/Covered Entity. OMIC agrees to abide by the assurances, terms, and conditions contained herein in the performance of its obligations as a Business Associate. This Agreement sets forth the manner in which PHI that is provided to, or received by, OMIC from the insured, or on behalf of the insured, will be handled. OMIC agrees as follows:

Section 1 Definitions

Unless otherwise provided, capitalized terms have the same meanings as set forth in the HIPAA Rules and HITECH Standards.

- 1.1 *Breach:*** "Breach" means the unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted under Part 164, Subpart E of the HIPAA Rules that compromises the security or privacy of such information, i.e. poses a significant risk of financial, reputational, or other harm to the individual. A breach does not occur where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information and as otherwise excepted in Section 13400(1)(B) of the HITECH Act and 42 CFR §164.402(2).
- 1.2 *Business Associate (BA):*** "Business Associate" (BA) means Ophthalmic Mutual Insurance Company (OMIC).
- 1.3 *Covered Entity (CE):*** "Covered Entity" (CE) means the insured.
- 1.4 *Designated Record Set:*** "Designated Record Set" means a group of records maintained by or for CE that is (1) the medical records and billing records about individuals maintained by or for CE, or (2) used, in whole or in part, by or for CE to make decisions about individuals. For the purposes of this paragraph, the term "Record" means any items, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for CE.

- 1.5 *Electronic Health Record (EHR):*** “Electronic Health Record” (EHR) means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.
- 1.6 *Electronic Protected Health Information (EPHI):*** “Electronic Protected Health Information” (EPHI) means Protected Health Information that is transmitted by or maintained in electronic media.
- 1.7 *HIPAA Rules:*** “HIPAA Rules” means the collective privacy and security regulations found at 45 CFR Parts 160 and 164, promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
- 1.8 *HITECH Standards:*** “HITECH Standards” means the privacy and security provisions applicable to Business Associates under Subtitle D of the Health Information Technology for Economic and Clinical Health Act, set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 (“HITECH Act”), and any regulations promulgated thereunder.
- 1.9 *Individual:*** "Individual" means the person who is the subject of protected health information and includes a person who qualifies as a personal representative in accordance with the HIPAA Rules and HITECH Standards.
- 1.10 *Protected Health Information (PHI):*** "Protected Health Information" (PHI) means certain individually identifiable health information, as defined in 45 CFR §160.103, limited to the information created or received by BA from or on behalf of CE. PHI includes Electronic Protected Health Information.
- 1.11 *Secretary:*** "Secretary" means the Secretary of the Department of Health and Human Services or his/her designee.
- 1.12 *Security Incident:*** “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.
- 1.13 *Unsecured Protection Health Information:*** “Unsecured Protection Health Information” or “Unsecured PHI” means PHI that is not secured through the use of a technology or methodology specified in the Secretary’s guidance or, if guidance is not available, PHI that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

Section 2

Obligations of Business Associate

BA agrees to the following:

- 2.1 *Limit PHI Use.*** BA agrees not to use PHI other than as permitted or required by the Agreement or as required or allowed by law.

- 2.2 *Limit PHI Disclosure.*** BA agrees not to disclose PHI except as permitted or required by this Agreement or as required by law. BA may disclose PHI (i) for BA's proper management and administration, and (ii) to carry out the legal responsibilities of BA under this Agreement, assuming either of the following are satisfied: (a) the disclosure is required by law or (b) BA obtains reasonable assurances from the person to whom BA further discloses the PHI that the information will be held confidentially, that the information will be used or further disclosed only as required by law or for the purposes for which it was disclosed, and the person notifies BA of any instances where the confidentiality of the information has been breached.
- 2.3 *Use Minimum Necessary.*** BA will takes reasonable efforts to limit request, use, and disclosure of PHI to the minimum necessary to accomplish the intended request, use, or disclosure, but only as required by the HIPAA Rules and HITECH Act Section 13405(b).
- 2.4 *Use Safeguards.*** BA agrees to use reasonable safeguards to prevent use or disclosure of PHI other than as allowed by this Agreement or as otherwise required or allowed by law. BA agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that BA creates, receives, maintains, or transmits on behalf of the insured.
- 2.5 *Report Inappropriate Uses or Disclosures of PHI.*** If BA becomes aware of any use or disclosure of PHI not permitted by this Agreement or by law, BA agrees to report such violation to CE.
- 2.6 *Report Security Incidents.*** If BA becomes aware of a Security Incident, BA agrees to report such incident to CE.
- 2.7 *Report Breaches of Unsecured PHI.*** In the event that BA discovers a Breach of Unsecured PHI, BA agrees to notify CE without unreasonable delay, and in no case later than 60 calendar days after BA first becomes aware of the incident, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. BA is deemed to have become aware of the Breach as of the first day on which such Breach is known or with the exercise of reasonable diligence would have been known to any person other than the person committing the Breach who is an employee, officer, or other agent of the BA. The notice must include the identification of the Individuals whose Unsecured PHI was the subject of the Breach; a brief description of what happened; the date of the Breach and the date of the discovery of the Breach, if known; a description of the types of Unsecured PHI that were involved in the Breach (such as full name, Social Security Number, date of birth, home address, account number, disability code, or types of information that were involved); any steps the Individuals should take to protect themselves from potential harm resulting from the Breach; a brief description of what CE and BA are doing to investigate the Breach, mitigate losses, and protect against further Breaches; and contact procedures for Individuals to ask questions or learn additional information, which must include a toll-free telephone number, email address, website, or postal address.
- 2.8 *Mitigate Harmful Effects.*** To the extent practicable, BA agrees to mitigate any harmful effects known to BA that are caused by the inappropriate use or disclosure of PHI or a Breach of Unsecured PHI.

- 2.9 *Require Compliance of Agents.*** BA agrees to require any agents, including subcontractors, to agree to the same restrictions and conditions that apply to BA throughout this Agreement, including implementing reasonable and appropriate safeguards to protect EPHI, provided that such agents perform a service that BA agreed to perform for, or on behalf of, CE under the Insurance Policy and provided that that BA provides PHI to such agents.
- 2.10 *Provide Access to Information.*** To the extent BA maintains the Designated Record Set, BA agrees to provide access to PHI in the original Designated Record Set, during normal business hours, provided CE or the Individual delivers prior written notice to BA, at least 20 days in advance of requesting such access, but only to the extent required by 45 CFR §164.524. If BA maintains an EHR, BA shall provide such information in electronic format to enable CE to fulfill its obligations under Section 13405(e) of the HITECH Act.
- 2.11 *Incorporate Amendments.*** Upon written request by CE or the Individual, to the extent BA maintains the Designated Record Set, BA agrees to incorporate any amendment(s) to PHI in the original Designated Record Set that CE approves, pursuant to 45 CFR §164.526.
- 2.12 *Make Available Information for Accounting of Disclosures.*** Upon written request by CE, BA agrees to make available to CE information concerning disclosure of PHI by BA or its agents that CE needs to provide an Individual with an accounting of disclosures of PHI in accordance with 45 CFR §164.528. To the extent required by BA under Section 13405(c) of the HITECH Act, if CE uses or maintains EHRs, BA will include in the accounting disclosures made for treatment, payment, or health care operations purposes through the EHR. BA agrees to make available to the Individual the information described above if properly requested by the subject Individual. Should an accounting of the PHI of a particular Individual be requested more than once in any twelve month period, BA may charge a reasonable, cost-based fee. BA shall have a reasonable time within which to comply with such requests and, in no case, shall access be required in less than 20 days after BA's receipt of such request. BA will maintain information in order to provide an Accounting going back a minimum of 6 years from the date of the request (3 years for accountings of disclosures from an EHR for treatment, payment, or health care operations purposes).
- 2.13 *Restrict Disclosure of PHI.*** Upon written request by CE on behalf of an Individual, BA agrees to consider restrictions on the use or disclosure of PHI agreed to by CE. BA will grant requests to limit disclosures to health plans for payment or health care operations purposes when the provider has been paid out of pocket in full for services or products as provided in Section 13405(a) of the HITECH Act.
- 2.14 *Restrict exchange of PHI with violators.*** BA will refrain from exchanging any PHI with any entity that the BA knows has a pattern of activity or practice that constitutes a material breach or violation of HIPAA.
- 2.15 *Use PHI As Permitted by Authorizations.*** Notwithstanding any other limitation in Section 2, BA agrees that nothing in this Agreement prohibits BA from using or

disclosing PHI to the extent permitted by an authorization from the appropriate Individual.

- 2.16 *Make Available Practices, Books, and Records.*** Unless otherwise protected or prohibited from discovery or disclosure by law, BA agrees to make internal practices, books, and records related to the use and disclosure of PHI received from CE or created or received by BA on behalf of CE available to the Secretary for purposes of determining BA's and CE's compliance with the HIPAA Rules and HITECH Standards. BA shall have a reasonable time within which to comply with such requests.

Section 3

Permitted Uses and Disclosures by Business Associate

- 3.1 *Purpose.*** Under the Insurance Policy, BA provides CE with insurance products and services, hereinafter "Services" that may involve the use and disclosure of PHI. Except as otherwise specified herein, BA may make any uses of PHI necessary to perform its obligations under this Agreement and under the Insurance Policy. Moreover, BA may disclose PHI for the purposes authorized by this Agreement: (i) to its employees, subcontractors, agents, and third parties in accordance with Sections 2 of this Agreement; or (ii) as otherwise permitted by the terms of this Agreement. All other uses not authorized by this Agreement are prohibited.
- 3.2 *Receipt and Use of PHI to Provide Services.*** The Executive, Administrative, Finance, Underwriting, Sales, Claims, Legal, Risk Management, and IT Departments of OMIC, and designated contractors, temporary employees, or other employees of OMIC may receive and use PHI, consisting of, but not limited to, records of patient history, diagnosis, treatment, and outcome, in order to provide Services to CE. Broadly, these Services include underwriting the Insurance Policy for determination of acceptance for coverage, processing of claims made under the Insurance Policy, and providing risk management services to holders of the Insurance Policy. Specifically, these Services may include, among others, receiving, evaluating, defending, and making payments related to incidents, claims, and lawsuits; quality assessment; quality improvement; loss prevention tools; outcomes evaluation; protocol and clinical guidelines development; reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance; conducting risk management programs to minimize the risk of malpractice claims against providers; arranging for legal services; conducting or arranging for audits to improve compliance; and other functions necessary to perform these Services.
- 3.3 *Disclosure of PHI to Provide Services.*** BA may disclose PHI to third parties, such as insurance service providers, settlement brokers, and third party administrators, in order to provide Services to CE.
- 3.4 *Use of PHI for Administration and Legal Responsibilities.*** BA may use PHI for the proper management and administration of BA or to carry out its legal responsibilities.
- 3.5 *Disclosure of PHI for Administration and Legal Responsibilities.*** BA may disclose PHI to third parties, such as copy and storage service providers, defense counsel, consultants, researchers, outside counsel, auditors, reinsurers, departments of insurance, and the

National Practitioner Data Bank, for the proper management and administration of BA and to carry out its legal responsibilities.

- 3.6** *Disclosure of PHI to Report Violations of the Law.* BA may disclose PHI to report violations of the law to law enforcement.
- 3.7** *Data Aggregation Services.* BA may use PHI to provide data aggregation services to CE as permitted by 45 CFR §164.504(e)(2)(i)(B).
- 3.8** *De-Identification.* BA may use PHI to create de-identified information consistent with the standards set forth at 45 CFR §164.514.
- 3.9** *Sales or Marketing.* BA shall not use or disclose PHI for fundraising or marketing purposes. BA shall not directly or indirectly receive remuneration in exchange for PHI, except with proper authorization or as otherwise permitted by the HITECH Act Section 13405(d). However this prohibition shall not affect payment by CE to BA for services provided pursuant to the Insurance Policy.

Section 4 **Impermissible Requests by CE**

BA understands that CE shall not request BA to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules or HITECH Standards if done by CE, except that, despite this Section 4, BA may use or disclose PHI for data aggregation or management and administrative activities of BA as is otherwise permitted by this Agreement.

Section 5 **Term and Termination**

- 5.1** *Term.* This Agreement is effective as of the date of execution above or when, thereafter, the insured joins OMIC as a member-insured and extends through the term of the Insurance Policy (including any extended reporting period) between BA and CE, and terminates when the term of the Insurance Policy (or extended reporting period) expires.
- 5.2** *Termination for Cause.* Upon one party's knowledge of a violation of a material term of the Agreement by the other party, the non-violating party shall provide an opportunity for the other party to cure the breach or end the violation. The non-violating party may terminate this Agreement if the violating party has violated a material term of this Agreement and cure is not possible. If termination is not feasible, the non-violating party must report the problem to the Secretary.
- 5.3** *Return of PHI at Termination.* Upon termination of the Agreement, BA shall, where feasible, destroy or return to CE all of the PHI provided by CE to BA, or created or received by BA on behalf of CE, in connection with the performance of BA's Services. If it is not feasible to return or destroy PHI, the duties of BA under the Agreement are extended to protect the PHI retained by BA. Notwithstanding any other limitation in this section, BA agrees that it is not necessary to return or destroy PHI received from, or created or received by BA on behalf of CE, if patient authorizations permitting such retention have been executed.

5.4 *Effect of Termination.* Upon termination of the Insurance Policy, the protections of this Agreement will remain in force and BA shall make no further use or disclosure of PHI except as required by law or for those purposes which made the return or destruction infeasible, including the proper management and administration of BA's business and carrying out BA's legal responsibilities.

Section 6 **General Provisions**

- 6.1** *Regulatory References.* A reference in this Agreement to a Section in the HIPAA Rules or HITECH Standards means the Section in effect or as amended, and for which compliance is required.
- 6.2** *Interpretation.* Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits compliance with the HIPAA Rules and HITECH Standards.
- 6.3** *Enforceability.* If any provision of this Agreement is held invalid or unenforceable, such invalidity or unenforceability attaches only to such provision and does not in any way affect or render invalid or unenforceable any other provision of this Agreement.
- 6.4** *Survival.* The rights and obligations of BA under this Agreement survive the termination of this Agreement and the termination of the Insurance Policy.
- 6.5** *Amendment.* BA, at its discretion, may amend this Agreement from time to time, to comply with HIPAA the HITECH Act, its amendments, regulations, or other federal laws that may be promulgated and affect the provisions of this Agreement.
- 6.6** *Communications.* All notices or communications required or permitted pursuant to the terms of this Agreement shall be in writing. All such notices will be deemed given upon delivery by service or in person, on the third business day after deposit with the U.S. Postal Service, or on the first business day after sending by facsimile or email. The BA may, at its discretion, post this Agreement and any Amendments to this Agreement on its website (www.omic.com) for the insured to read and download, instead of mailing or otherwise delivering a copy of this Agreement or Amendments to the insured.

On Behalf of Ophthalmic Mutual Insurance Company



Signature:

By: Kimberly Wynkoop

Title: Legal Counsel