

## **Business Associate Agreement Between KaMMCO and KaMMCO Insureds**

THIS AGREEMENT and commitment is executed by Kansas Medical Mutual Insurance Company (KaMMCO).

### **Recitals**

KaMMCO and its insureds, who are health care providers, have an insurer/insured relationship by virtue of insurance policies issued by KaMMCO to the insured, hereinafter, "Insurance Policies." Because of its relationship with its insureds, there may be instances in which KaMMCO may be considered a business associate of its insureds. KaMMCO is committed to complying with the Standards for Security and Privacy of Individually Identifiable Health Information (the "Security and Privacy Regulations"), as applicable, under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended, as well as with the Health Information Technology for Economic and Clinical Health Act (HITECH), 42 U.S.C. §§17921-53, enacted as part of the America Recovery and Reinvestment Act of 2009. Under the Security and Privacy Regulations, many KaMMCO insureds are "covered entities." 45 C.F.R. §160.103. KaMMCO, in conducting certain activities on behalf of its insureds, may be deemed a business associate of its insureds. 45 C.F.R. §164.502(e) and 45 C.F.R. §164.504(e). KaMMCO uses and discloses protected health information in its performance of insurance related functions and services to its insureds. To the extent KaMMCO is deemed a business associate of its insureds, KaMMCO agrees to abide by the assurances, terms, and conditions contained herein in the performance of its services for its insureds. This Business Associate Agreement (Agreement) sets forth the authorized uses and disclosures of Protected Health Information that is created, received, maintained, or transmitted by KaMMCO from its insured, or on behalf of its insureds, will be handled. KaMMCO agrees as follows:

### **Section 1 Definitions**

As used throughout this Agreement, the following terms shall have the meaning set forth below regardless of whether such term is capitalized:

- 1.1 *Business Associate.*** "Business Associate" shall mean KaMMCO to the extent KaMMCO meets the definition of "business associate", as defined in 45 C.F.R. §160.103.
- 1.2 *Covered Entity.*** "Covered Entity" shall mean a KaMMCO insured.
- 1.3 *Designated Record Set.*** "Designated Record Set" shall have the same meaning as the term "Designated Record Set" in 45 C.F.R. §164.501.
- 1.4 *Electronic Protected Health Information (E-PHI).*** "E-PHI" shall have the same meaning as the term, "Protected Health Information" in 45 C.F.R. §160.103,

limited to information transmitted by, or maintained in, electronic media received by Business Associate from, or on behalf of, Covered Entity.

- 1.5 **HIPAA.** "HIPAA" shall mean the administrative simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) and shall include 45 C.F.R. Part 160 and 45 C.F.R. Part 164.
- 1.6 **HIPAA Privacy Rule.** "HIPAA Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and 45 C.F.R. Part 164 and will include relevant portions of HITECH.
- 1.7 **HIPAA Security Rule.** "HIPAA Security Rule" shall mean the Security Standards for protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and 45 C.F.R. Part 164, subparts A and C and shall include HITECH.
- 1.8 **HITECH.** "HITECH" shall mean the Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§17921-17953 enacted as part of the America Recovery and Reinvestment Act of 2009.
- 1.9 **Individual.** "Individual" shall have the same meaning as the term "Individual" in 45 C.F.R. §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502(g).
- 1.10 **Insurance Policy/Policies.** "Insurance Policy" and "Insurance Policies" shall mean the insurance policy and/or policies that exist between KaMMCO and a particular KaMMCO insured.
- 1.11 **Protected Health Information (PHI).** "Protected Health Information" and "PHI" shall have the same meaning as the term "Protected Health Information" in 45 C.F.R. §160.103 and includes E-PHI.
- 1.12 **Secretary.** "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.
- 1.13 **Security Incident.** "Security Incident" shall have the same meaning as the term "Security Incident" in 45 C.F.R. §164.304.
- 1.14 **Subcontractor.** "Subcontractor" shall have the same meaning as the term "subcontractor" is defined in 45 C.F.R. §160.103.
- 1.15 **Unsecured Protected Health Information.** "Unsecured Protected Health Information" shall have the same meaning as the term "Unsecured Protected Health Information" in 45 C.F.R. §164.402.

**Section 2**  
**Obligations and Activities of Business Associate**

**2.1 *Permitted or Required Use or Disclosure of PHI /Restriction Requests/Marketing.***

- a) Business Associate agrees not to use, or further disclose, Protected Health Information ("PHI") other than as permitted or required by this Agreement or as required or allowed by law.
- b) Business Associate will not use or disclose PHI for fundraising or marketing purposes except as authorized by law.
- c) To the extent applicable and to the extent required by HIPAA and/or HITECH, at the request of an individual, Business Associate agrees to limit disclosure to health plans of an Individual's PHI for purposes of payment or health care operations if the PHI pertains solely to a health care item or service for which the involved health care providers have been paid out-of-pocket in full.
- d) To the extent Business Associate is to carry out a Covered Entity's obligation under the HIPAA Privacy Rule and/or HIPAA Security Rule, as amended by HITECH, Business Associate will comply with the requirements of the HIPAA Privacy Rule and/or the HIPAA Security Rule that apply to Covered Entity in the performance of such obligation.

**2.2 *Safeguards/HIPAA Security Rule/Minimum Necessary.***

- a) Business Associate agrees to use reasonable safeguards to prevent use or disclosure of the PHI other than as allowed by this Agreement or as otherwise required or allowed by law. Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably protect the confidentiality, integrity, and availability of E-PHI that Business Associate creates, receives, maintains, or transmits from, or on behalf of, the Covered Entity. Business Associate will strive to comply with 45 C.F.R. 164.308, 164.310, 164.312, and 164.316 of the HIPAA Security Rule as required by HITECH.
- b) Absent an applicable exception to the minimum necessary rule as set forth in the HIPAA Privacy Rule, as amended by HITECH, Business Associate will strive to limit use, disclosure, and requests of, PHI to the minimum necessary (as defined by HIPAA and HITECH) to accomplish intended purpose of the use or disclosure.

**2.3 *Mitigation of Harmful Effects.*** Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use

or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

**2.4 *Reporting of Security Incidents and Breach of PHI/Unauthorized Use or Disclosure.***

- a) Business Associate agrees to report to Covered Entity any use or disclosure of PHI not permitted by this Agreement or by law. Business Associate agrees to report to the Covered Entity any Security Incident related to E-PHI of which Business Associate becomes aware.
- b) Business Associate agrees to notify Covered Entity of any breach of PHI by Business Associate as “breach” is defined by 45 C.F.R. §164.402 pertaining to unsecured PHI without unreasonable delay and in no case later than 60 days after discovery of such breach by Business Associate and as required by 45 C.F.R. §164.410.

**2.5 *Subcontractors.*** To the extent required by the HIPAA/HITECH, Business Associate agrees to require any subcontractors that create, receive, maintain, or transmit PHI from, or on behalf of, Business Associate to agree to the same restrictions and conditions set forth in this Agreement that apply to Business Associate with respect to PHI. Business Associate agrees to require any subcontractors to whom it provides E-PHI, to agree to implement the reasonable and appropriate safeguards to protect E-PHI that are required by law, including but not limited to the safeguards set out in the HIPAA Security Rule, HIPAA Privacy Rule, and HITECH.

**2.6 *Access.*** To the extent the Business Associate maintains the Designated Record Set, Business Associate agrees to provide access to PHI in the original Designated Record Set, during normal business hours, provided the Covered Entity delivers prior written notice to the Business Associate, at least fifteen business days in advance, requesting such access, but only to the extent required by 45 C.F.R. §164.524.

**2.7 *Amendments.*** To the extent the Business Associate maintains the Designated Record Set, Business Associate agrees to incorporate any amendment(s) to PHI in the original Designated Record Set that the Covered Entity directs, pursuant to 45 C.F.R. §164.526.

**2.8 *Disclosure of Practices, Books, and Records.*** Unless otherwise protected or prohibited from discovery or disclosure by law, Business Associate agrees to make internal practices, books, and records related to the use and disclosure of PHI created, received, maintained, or transmitted by the Business Associate, from, or on behalf of, the Covered Entity available to the Secretary for purposes of determining compliance with the HIPAA Privacy Rule, the HIPAA Security Rule, and HITECH. Business Associate shall have a reasonable time within which to comply

with such requests and, in no case, shall access be required in less than fifteen business days after the Business Associate's receipt of such request.

**2.9 Accounting.**

- a) Business Associate agrees to maintain sufficient documentation to allow Business Associate to provide to Covered Entity a list of any disclosures of PHI by the Business Associate so as to allow the Covered Entity, or, when appropriate, the Business Associate, to provide an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528.
- b) To the extent applicable, if Business Associates makes a disclosure of PHI through an electronic health record for payment, treatment, or health care operations, Business Associate will include such disclosure on an accounting in addition to maintaining an accounting of those other disclosures required by the HIPAA Privacy Rule under 45 C.F.R. § 164.528. To the extent applicable and required by the HIPAA Privacy Rule and HITECH, Business Associate will provide an accounting of disclosures made through an electronic health record for payment, treatment, or health care operations.

**2.10 Release of Documentation of Certain Disclosures.** Business Associate agrees to provide to Covered Entity information collected in accordance with Section 2.9 of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528 and HITECH. Business Associate shall have a reasonable time within which to comply with such requests and, in no case shall access be required in less than fifteen business days after the Business Associate's receipt of such request.

**2.11 Security and Privacy Requirements of HIPAA/HITECH.** In addition to the commitments made herein expressly, Business Associate will strive to comply with any other additional security or privacy requirements of HIPAA and HITECH applicable to Business Associate.

### **Section 3**

#### **Permitted Uses and Disclosures by Business Associates**

**3.1 Use of PHI for Specified Purposes.** Pursuant to its insurer/insured relationship, the Business Associate provides the Covered Entity with insurance products and services, hereinafter "Services," that involve the use and disclosure of PHI. These Services may include, among others, the provision of insurance, including but not limited to professional, general, and cyber liability insurance; receiving and evaluating 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 training programs to improve the skills of health care practitioners and providers;

credentialing, conducting or arranging for medical review; arranging for legal services; conducting or arranging for audits to improve compliance; resolution of internal grievances; placing stop-loss and excess of loss insurance; and other functions necessary to perform these Services. Except as otherwise specified herein, the Business Associate may make any use of PHI necessary to perform the Services and to perform its obligations under this Agreement and under the Insurance Policies. Moreover, the Business Associate may disclose PHI for the purposes authorized by this Agreement: (i) to its employees, subcontractors, agents, representatives, and to third parties as allowed or required by law or by this Agreement; or (ii) as otherwise permitted by the terms of this Agreement. All other uses not authorized by this Agreement or by the law are prohibited.

- 3.2 *Use of PHI for Business Associate's Management and Administration/Legal Responsibilities.*** Business Associate may use PHI for the proper management and administration of the Business Associate and to carry out the legal responsibilities of the Business Associate.
- 3.3 *Disclosure Required by Law or With Reasonable Assurances.*** Business Associate may disclose PHI ("PHI") for the proper management and administration of the Business Associate, to carry out the legal responsibilities of the Business Associate, and to carry out the Services described in 3.1 and its related responsibilities, provided that disclosures are required or allowed by law, or provided that the Business Associate obtains the following reasonable assurances from the person or entity to whom the Protected Health Information is disclosed: 1) the PHI will remain confidential; 2) the PHI will be used or further disclosed only as required or allowed by law or for the purposes for which it was disclosed; and, 3) the person or entity will notify the Business Associate of any instances of which the person or entity is aware in which the confidentiality of the information has been breached.
- 3.4 *Data Aggregation Services.*** Business Associate may use PHI to provide data aggregation services relating to the health care operations of the Covered Entity as permitted by 45 C.F.R. §164.504(e)(2)(i)(B).
- 3.5 *Use/Disclosure Authorized by the Privacy Rule.*** In accordance with 45 C.F.R. §164.504(e)(2), Business Associate will not use or disclose PHI in any manner that would violate the requirements of the HIPAA Privacy Rule if done by the Covered Entity, except that, as provided in this Agreement, the Business Associate may use and disclose PHI for the proper management and administration of the Business Associate as allowed by 45 C.F.R. §164.504(e)(4) and for Data Aggregation Services as set forth in Section 3.4 of this Agreement.

**Section 4**  
**Impermissible Requests by Covered Entity**

Business Associate understands that the Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule or HIPAA Security Rule if done by Covered Entity, except that, despite this Section 4, Business Associate may use or disclose PHI for data aggregation, for management and administrative activities of Business Associate, and as is otherwise permitted or required by this Agreement or the law.

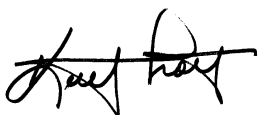
**Section 5**  
**Term and Termination**

- 5.1** *Term.* The term of this Agreement shall be effective during the terms of the Insurance Policies that exist between KaMMCO and its insureds on or after September 11, 2013. This agreement shall terminate when all of the PHI created, received, maintained, or transmitted by Business Associate, from, or on behalf of, Covered Entity is destroyed or returned to Covered Entity, or, if it is not feasible to return or destroy PHI, upon the application of the protections described in 5.2 of this Agreement.
- 5.2** *Destruction/Return of PHI/ Extension of Protections.* At the termination of the Agreement, if feasible, Business Associate shall return or destroy all PHI created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity in any form and retain no copies of such PHI. If such return or destruction is not feasible, Business Associate agrees to extend the protections of this Agreement to such PHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
- 5.3** *Termination for Cause.* Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation. Covered Entity may terminate this Agreement, and Business Associate agrees to such immediate termination, if Business Associate has breached a material term of this Agreement and cure or ending of the violation is not possible.
- 5.4** *Effect of Termination.* Upon termination of this Agreement, the protections of this Agreement will remain in force and Business Associate shall make no further uses and disclosures of PHI except for the proper management and administration of its business or to carry out its legal responsibilities or as required by law.

**Section 6**  
**Miscellaneous Provisions**

- 6.1** *Regulatory References.* A reference in this Agreement to a section in the HIPAA Privacy Rule, HIPAA Security Rule, HIPAA, or HITECH means the section in effect at the time compliance is required.
- 6.2** *Amendment.* The Business Associate agrees to take such action as is necessary to amend this Agreement from time to time as necessary, as determined by the Business Associate, for compliance with the requirements of the HIPAA Privacy Rule, HIPAA Security Rule, HIPAA, HITECH, or other provision in the law as determined by the Business Associate.
- 6.3** *Survival.* The rights and obligations of Business Associate under this Agreement shall survive the termination of this Agreement and the termination of the Insurance Policies.
- 6.4** *Interpretation.* Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Privacy Rule, the HIPAA Security Rule, HIPAA, and HITECH.

**KaMMCO**



Kurt Scott  
President and Chief Executive Officer  
Date: September 11, 2013