

April 21, 2005

Re: Business Associate Agreement
HIPAA Privacy and Security Rule Compliance

Dear Policyholder:

As you are aware, physicians and others involved in the delivery of healthcare to patients must achieve and maintain compliance with Privacy and Security regulations that implement the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) on and after the Security compliance date of April 21, 2005. Under HIPAA’s Privacy and Security Rules, MAG Mutual Insurance Company is considered a “business associate” of the physicians that we insure for medical professional liability coverage.

HIPAA regulations require covered entities such as physicians to obtain contractual assurance as to how their business associates handle patient health information. In this regard, enclosed you will find a Business Associate Agreement provided for you by MAG Mutual that has been updated to reflect HIPAA Security Rule and Privacy Rule requirements. This document replaces that Business Associate Agreement previously provided to you that addressed only the Privacy Rule requirements. MAG Mutual may never receive patient health information from many of its policyholders. However, to the extent that we may receive such information from you, this document outlines what MAG Mutual will and will not do with that information, and covers our commitment not to use or disclose it except as required or permitted by law or the Agreement.

There is no need for you to sign the Business Associate Agreement. However, you should keep the Agreement with other documentation that proves your compliance with the HIPAA Privacy and Security Rules. Please forward these materials to the HIPAA privacy officer, security officer or compliance officer in your practice.

Sincerely,



Thomas M. Gose
President
MAG Mutual Insurance Company

BUSINESS ASSOCIATE AGREEMENT
HIPAA Privacy and Security Rules

THIS AGREEMENT and commitment is executed by MAG Mutual Insurance Company effective the 21st day of April 2005, and shall replace any Business Associate Agreement previously executed by MAG Mutual Insurance Company in favor of its policyholder.

MAG Mutual Insurance Company and its policyholder have an insurer/insured relationship by virtue of a professional liability insurance policy issued by MAG Mutual that covers the policyholder (“Insurance Policy”). MAG Mutual and its policyholder are committed to complying with the Privacy Rule and Security Rule (45 C.F.R. Parts 160, 162 and 164) under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Under the Rules, the policyholder is a “covered entity” and MAG Mutual is a “business associate” of the policyholder. MAG Mutual must use and/or disclose Protected Health Information in its performance of services under the Insurance Policy, and HIPAA permits the policyholder to disclose such information to MAG Mutual for the activities set forth herein. MAG Mutual agrees to abide by the assurances, terms, and conditions contained herein. This Agreement sets forth the manner in which Protected Health Information that is provided to, or received by, MAG Mutual from or on behalf of the policyholder will be handled and protected. MAG Mutual agrees as follows:

Section 1
Definitions

- 1.1 “*Business Associate*” shall mean MAG Mutual Insurance Company.
- 1.2 “*Covered Entity*” shall mean the MAG Mutual Insurance Company policyholder and any persons covered under the policyholder’s Insurance Policy.
- 1.3 “*Designated Record Set*” shall have the same meaning as the term “Designated Record Set” in 45 C.F.R. §164.501.
- 1.4 “*Individual*” shall have the same meaning as the term “Individual” in 45 C.F.R. §164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502.
- 1.5 “*Protected Health Information*” (PHI) shall have the same meaning as the term “Protected Health Information” in the Security and Privacy Rules, limited to the information received by Business Associate from, or on behalf of, Covered Entity.
- 1.6 “*Electronic Protected Health Information*” shall have the same meaning as the term “Electronic Protected Health Information” in 45 C.F.R. §160.103.

Section 2
Obligations and Activities of Business Associate

Business Associate agrees to the following:

- 2.1 ***Not to Use or Disclose PHI Unless Permitted.*** Business Associate agrees not to use, or further disclose, Protected Health Information other than as permitted or required by this Agreement or as required or allowed by law.

- 2.2 ***Use Safeguards.*** Business Associate agrees to use reasonable safeguards to prevent use or disclosure of the Protected Health Information other than as allowed by this Agreement or as otherwise required or allowed by law.
- 2.3 ***Report Inappropriate Disclosures of PHI.*** Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not permitted by this Agreement or by law, of which it becomes aware.
- 2.4 ***Compliance of Agents.*** Business Associate agrees to require any agents, including subcontractors, to agree to the same restrictions and conditions that apply to Business Associate through this Agreement, provided that such agents perform a service that the Business Associate agreed to perform for, or on behalf of, the Covered Entity under the Insurance Policy and, to whom the Business Associate provides Protected Health Information.
- 2.5 ***Access.*** In the event that Business Associate maintains the Designated Record Set, Business Associate agrees to provide Covered Entity access to Protected Health Information in the Designated Record Set, during normal business hours, provided the Covered Entity delivers prior written notice to the Business Associate, at least five business days in advance, requesting such access but only to the extent required by 45 C.F.R. §164.524.
- 2.6 ***Amendments.*** In the event that Business Associate maintains the Designated Record Set, Business Associate agrees to incorporate any amendment(s) to Protected Health Information in the Designated Record Set that the Covered Entity directs, pursuant to 45 C.F.R. §164.526.
- 2.7 ***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 available to the Covered Entity or to the Secretary of the U.S. Department of Health & Human Services or his/her designee, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule but only to the extent such access is related to the use and disclosure of Protected Health Information received from the Covered Entity, or created or received by Business Associate on behalf of Covered Entity. 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 five business days after the Business Associate's receipt of such request.
- 2.8 ***Accounting.*** Business Associate agrees to maintain sufficient documentation to allow it to provide to Covered Entity a list of any disclosures of Protected Health Information by the Business Associate or its agents so as to allow the Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528.
- 2.9 ***Release of Documentation of Disclosures.*** Business Associate agrees to provide to Covered Entity information collected in accordance with Section 2.8 of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528. 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 five business days after the Business Associate's receipt of such request.
- 2.10 ***Security of Electronic Protected Health Information.*** Business Associate agrees to implement Administrative, Physical and Technical Safeguards, all as defined in 45 C.F.R. §164.304, that reasonably and appropriately protect the confidentiality, integrity, and availability of any Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf

of Covered Entity, as required by the Security Rule. Business Associate shall ensure that any agent, including a subcontractor to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it. Business Associate shall also report to Covered Entity any Security Incident, as defined in 45 C.F.R. §164.304, of which it becomes aware regarding the Protected Health Information.

Section 3 **Permitted Uses and Disclosures by Business Associates**

- 3.1 ***Use of PHI for Specified Purposes.*** Under the Insurance Policy, the Business Associate provides the Covered Entity with insurance products and services, hereinafter “Services,” that involve the use and disclosure of Protected Health Information, which may include Electronic Protected Health Information. These Services may include, among others, the provision of professional liability insurance; receiving and evaluating incidents, claims, and lawsuits; risk management; 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 healthcare 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 uses of Protected Health Information necessary to perform its obligations under this Agreement and under the Insurance Policy. Moreover, the Business Associate may disclose Protected Health Information for the purposes authorized by this Agreement: (a) to its employees, subcontractors, and agents, in accordance with paragraphs 3.2 through 3.4 of this Section below; or (b) as otherwise permitted by the terms of this Agreement or by law. All other uses not authorized by this Agreement or by law are prohibited.
- 3.2 ***Use of PHI for Business Associate Management and Administration.*** Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- 3.3 ***Disclosure Required by Law or With Reasonable Assurances.*** Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate and to carry out its legal responsibilities, provided that disclosures are required 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: (a) the PHI will remain confidential; (b) the PHI will be used or further disclosed only as required by law or for the purposes for which it was disclosed; and (c) 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 Protected Health Information to provide data aggregation services to Covered Entity as permitted by 45 C.F.R. §164.504.

Section 4 **Impermissible Requests by Covered Entity**

Business Associate understands that the Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except that, Business Associate may use or disclose Protected Health

Information for data aggregation or management and administrative activities of Business Associate as is otherwise permitted by law or by this Agreement.

Section 5 **Term and Termination**

- 5.1 **Term.** The term of this Agreement shall be effective during the term of the Insurance Policy between the Business Associate and the Covered Entity and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is not feasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.
- 5.2 **Termination for Cause.** Upon Covered Entity's knowledge of a material breach by Business Associate of this Agreement, 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 is not possible.
- 5.3 **Effect of Termination.** Upon termination of the Insurance Policy, the protections of this Agreement will remain in force and Business Associate shall make no further uses and disclosures of Protected Health Information 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 Privacy or Security Rule means the Section in effect or as amended, and for which 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 is necessary, as determined by the Business Associate, for compliance with requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act, as determined by the Business Associate.
- 6.3 **Survival.** The rights and obligations of Business Associate under this Agreement shall survive the termination of the Agreement and the termination of the Insurance Policy.
- 6.4 **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy and Security Rules.

MAG Mutual Insurance Company



Thomas M. Gose, President
MAG Mutual Insurance Company