

April 21, 2005

**Re: NORCAL Offers Assistance with Your HIPAA Compliance**

Dear Policyholder,

As you may know, the new federal security provisions of the *Health Insurance Portability and Accountability Act* (HIPAA) go into effect on April 21, 2005.

If you engage in the electronic management and distribution of patients' protected health information, you are considered a *Covered Entity* under HIPAA and thus required to have a Business Associate Agreement with NORCAL.

We previously sent out Business Associate Agreements to our insureds when the HIPAA privacy regulations took effect in April 2003. We are posting our newly modified Business Associate Agreement, which incorporates the new security rule, on our internet site for your convenience. The posted Agreement satisfies the requirement that your "Business Associates"—in this case NORCAL—provide a written assurance that they will abide by HIPAA guidelines.

**You do not need to do anything except download the Agreement, then file it with the other documents relating to your NORCAL coverage or in your files regarding HIPAA compliance.**

Please note, the Agreement does not modify or supersede any of the terms or conditions of your insurance policy with NORCAL, nor does it satisfy the requirement of your other Business Associates to provide their own modified or revised Business Associate Agreements. You should follow up with your other Business Associates individually to ensure that they also provide proper documentation assuring HIPAA compliance.

For more information on HIPAA, please visit our website at [www.norcalmutual.com](http://www.norcalmutual.com) and read the November/December 2002 issue of *Claims Rx*. If you require additional information about the Business Associate Agreement, or if you have any other questions about your policy, please call the Policyholder Services Unit at (877) 443-7232.

Sincerely,



James Sunseri  
President & Chief Executive Officer



THIS AGREEMENT and commitment is executed this 20th day of April 2005, by NORCAL Mutual Insurance Company, hereinafter referred to as “NORCAL.” This agreement supersedes inconsistent provisions of existing agreements between the parties.

NORCAL and the insured or applicant have an insurer/insured relationship by virtue of a professional liability policy requested from or issued by NORCAL. NORCAL and its insureds and applicants are committed to complying with the Standards for Privacy of Individually Identifiable Health Information (the “Privacy Regulations”) and Security Regulations under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Under the Privacy Regulations, the NORCAL insured or applicant may be a “Covered Entity,” and, as defined by 45 C.F.R. §164.502(e) and 45 C.F.R. §164.504(e), NORCAL may be a “Business Associate” of the insured or applicant. This Agreement sets forth the manner in which NORCAL will handle “Protected Health Information” that is provided by or received from or on behalf of the insured or applicant. NORCAL agrees as follows:

## **SECTION 1**

### *Definitions*

**1.1 Business Associate:** “Business Associate” shall mean a “Business Associate” as defined in 45 C.F.R. §164.501. Unless otherwise specified, the term Business Associate in this Agreement shall refer to NORCAL.

**1.2 Covered Entity:** “Covered Entity” shall mean the insured or applicant.

**1.3 Designated Record Set:** “Designated Record Set” means “Designated Record Set” as defined in 45 C.F.R. §164.501.

**1.4 Electronic Protected Health Information:** “Electronic Protected Health Information” shall mean Protected Health Information that is transmitted or maintained in electronic format or by electronic media.

**1.5 Insurance Policy:** “Insurance Policy” shall mean the policy of professional liability insurance requested by an applicant or now in effect between NORCAL and the insured, and any subsequent or replacement policy between NORCAL and the insured.

**1.6 Privacy Rule:** “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. parts §160 and §164, subparts A and E, as amended from time to time.

**1.7 Protected Health Information (PHI):** “Protected Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information” in 45 C.F.R.



§164.501, limited to the information received by NORCAL from, or on behalf of, Covered Entity.

**1.8 Secretary:** “Secretary” shall mean the Secretary of the Department of Health and Human Services of his/her designee.

**1.9 Security Incident:** “Security Incident” shall have the same meaning as the term “Security Incident” in 45 C.F.R. §164.304.

**1.10 Security Rule:** “Security Rule” shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. §160 and §164, subparts A and C.

## **SECTION 2**

### *Obligations and Activities of NORCAL*

In consideration of the Covered Entity’s continuing obligation to assist and cooperate with NORCAL’s efforts in providing services under the Insurance Policy, NORCAL hereby agrees to the following:

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

**2.2 Use Safeguards.** NORCAL agrees to use reasonable safeguards to prevent use or disclosure of Protected Health Information other than as allowed by this Agreement or as otherwise required or allowed by law. NORCAL will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of any Electronic Protected Health Information NORCAL creates, receives, maintains or transmits on behalf of Covered Entity.

**2.3 Mitigation of Harmful Effects.** NORCAL agrees to mitigate, to the extent practicable, any harmful effect that is known to NORCAL of a use or disclosure of Protected Health Information by NORCAL in violation of the requirements of this Agreement.

**2.4 Report Inappropriate Disclosure of PHI.** NORCAL agrees to report to Covered Entity any use or disclosure of the Protected Health Information not permitted or required by this Agreement of which NORCAL becomes aware. NORCAL also agrees to report to Covered Entity any Security Incident related to Electronic Protected Health Information of which NORCAL becomes aware.

**2.5 Compliance of Agents.** NORCAL agrees to require any agents, including subcontractors, to agree to the same restrictions and conditions that apply to NORCAL through



this Agreement provided that such agents perform a service that NORCAL agreed to perform for, or on behalf of, the Covered Entity under the Insurance Policy and to whom NORCAL provides Protected Health Information. NORCAL also agrees to ensure that any agent, including a subcontractor, to whom it provides Electronic Protected Health Information agrees to implement reasonable and appropriate safeguards to protect it.

**2.6 Access.** To the extent that NORCAL possesses a Designated Record Set, NORCAL agrees to provide access to the Protected Health Information in that Designated Record Set, during normal business hours, provided the Covered Entity delivers prior written notice to NORCAL, at least five 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 that NORCAL possesses a Designated Record Set, NORCAL agrees to incorporate any amendment(s) to Protected Health Information in that 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 from discovery or disclosure by law or unless otherwise prohibited from discovery or disclosure by law, NORCAL agrees to make internal practices, books, and records available to the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule. NORCAL 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 NORCAL's receipt of such request.

**2.9 Accounting.** NORCAL agrees to maintain sufficient documentation to allow it to provide to Covered Entity a list of any disclosures of Protected Health Information by NORCAL 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.

### **SECTION 3**

#### *Permitted Uses and Disclosures by NORCAL*

**3.1 Use of PHI for Specified Purposes.** Under the Insurance Policy, NORCAL provides the Covered Entity with insurance products and services (hereinafter "Services") that involve the use and disclosure of Protected Health Information as defined by the Privacy Regulations. These Services may include, among others, the acceptance, declination, or acceptance with revisions of professional 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 insurance or reinsurance, including but not limited to pro rata, stop-loss, and excess of loss insurance, and other functions necessary to perform these Services. NORCAL may make any uses of Protected Health Information necessary to perform its obligations under this Agreement and under the Insurance Policy. Moreover, NORCAL may disclose Protected Health Information for the purposes authorized by this Agreement: (i) to its employees, subcontractors, and agents, in accordance with paragraphs Section 3.2 through 3.4 of this Section below; or (ii) as otherwise permitted by the terms of this Agreement. All other uses not authorized by this Agreement are prohibited.

**3.2 Use of PHI for NORCAL Management and Administration.** NORCAL may use Protected Health Information for the proper management and administration of NORCAL or to carry out the legal responsibilities of NORCAL.

**3.3 Disclosure Required by Law or With Reasonable Assurance.** NORCAL may disclose Protected Health Information for the proper management and administration of NORCAL and to carry out its legal responsibilities, provided that disclosures are required by law, or provided that NORCAL 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 by law or for the purposes for which it was disclosed; and 3) the person or entity will notify NORCAL 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.** NORCAL may use Protected Health Information to provide data aggregation services to Covered Entity as permitted by 45 C.F.R. §164.504(e)(2)(i)(B).

**3.5 De-identified Information.** NORCAL may de-identify any and all Protected Health Information in accord with the requirements of applicable law as provided in 42 C.F.R. §164.514(b), and use or disclose all such de-identified information for its own managerial and administrative activities as it sees fit. NORCAL agrees to maintain such documentation regarding de-identified information as required by 42 C.F.R. §164.514(b). Covered Entity understands and acknowledges that de-identified information is not Protected Health Information under the terms of this Agreement.



## **SECTION 4**

### *Impermissible Requests by Covered Entity*

NORCAL shall not 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, despite this Section 4, NORCAL may use or disclose Protected Health Information for data aggregation or management and administrative activities of NORCAL as provided in sections 3.2, 3.3, and 3.4 above, or as otherwise permitted by this Agreement.

## **SECTION 5**

### *Term and Termination*

**5.1 Term.** This Agreement shall remain effective during the time that NORCAL provides the Covered Entity with Services, as defined in section 3.1 above, pursuant to the terms of the Insurance Policy, and shall terminate when all such Services under the Insurance Policy are terminated and all of the Protected Health Information created or received by NORCAL on behalf of Covered Entity is destroyed or returned to Covered Entity; provided, however, certain provisions and requirements of this Agreement shall survive such termination in accord with subsection 5.3, below.

**5.2 Termination by Covered Entity.** Upon Covered Entity's determination that NORCAL has breached a material term of this Agreement, Covered Entity shall immediately notify NORCAL and provide NORCAL a reasonable opportunity to cure the breach. Covered Entity may terminate this Agreement, and NORCAL agrees to such immediate termination, if NORCAL has breached a material term of this Agreement and cure is not possible. **Covered Entity and NORCAL hereby acknowledge and agree that the termination of this Agreement by Covered Entity shall have no effect on the terms and conditions of the Insurance Policy between them unless NORCAL determines, in its sole discretion, that the termination of this Agreement by Covered Entity constitutes a breach of Covered Entity's duty of cooperation under the Insurance Policy.**

**5.3 Effect of Termination.** Upon termination of NORCAL's provision of Services under the Insurance Policy, the protection of this Agreement will remain in force and NORCAL 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. To the extent that it is feasible to do so, NORCAL agrees to return or destroy all PHI, pursuant to 45 C.F.R. §164(e)(2)(ii)(I), and to require any and all of its subcontractors or agents to return or destroy any PHI in their possession. However, NORCAL and Covered Entity hereby acknowledge and agree that, because of the nature of the Services provided by NORCAL and its business obligations, it is not feasible to return or destroy all



Protected Health Information immediately on the termination of this Agreement, or for some time thereafter. Therefore, NORCAL agrees to extend, and require its subcontractor and agents to extend, and all protections, limitations, and restrictions contained in this Agreement to such PHI as may be retained after the termination of this Agreement. **This section 5 shall survive the termination of this Agreement and NORCAL's provision of Services under the Insurance Policy.**

## **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.** NORCAL agrees to take such action as is necessary to amend this Agreement from time to time as is necessary, as determined by NORCAL, for compliance with the requirements of the Privacy Rule, the Security Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191 as determined by NORCAL.

A handwritten signature in black ink that reads "David R. Holley, MD." The signature is fluid and cursive.

David R. Holley, MD  
Secretary, Board of Directors

A handwritten signature in black ink that reads "James Sunseri". The signature is fluid and cursive.

James Sunseri  
President & Chief Executive Officer