

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Hereinafter "**Agreement**") dated as of _____ is made by and between Community Memorial Health System, a California not-for-profit corporation (Hereinafter "**Covered Entity**") and _____ (Hereinafter "**Business Associate**" – only if deemed a Business Associate).

ARTICLE 1 INTRODUCTION

1.1 This Agreement governs the terms and conditions under which Business Associate will access Protected Health Information belonging to patients of Covered Entity in performing services for, or on behalf of, Covered Entity. Specifically, this agreement governs the terms and conditions under which Business Associate will provide _____ (Hereinafter, "**Services**").

1.2 Covered Entity and Business Associate intend to: (a) protect the privacy and provide for the security of Protected Health Information disclosed pursuant to this Agreement and (b) comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), Public Law 111-5, and the regulations promulgated thereunder by the U.S. Department of Health & Human Services (Hereinafter, "**HIPAA Regulations**"), and other applicable federal and state laws.

ARTICLE 2 DEFINITIONS

2.1 Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Regulations.

2.2 For purposes of this Agreement:

2.2.1 "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under Subpart E of 45 CFR Part 164 that compromises the security or privacy of the PHI (within the meaning of 45 CFR 164.402).

2.2.2 "Designated Record Set" shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR 164.501.

2.2.3 "Electronic Protected Health Information" or "ePHI" means PHI that is transmitted by or maintained in electronic media as defined in 45 CFR 160.103.

2.2.4 "Individual" shall have the same meaning as the term "Individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

2.2.5 "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, subparts A and E.

2.2.6 "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

2.2.7 “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR 164.501.

2.2.8 “Secretary” shall mean the Secretary of the Department of Health and Human Services or his/her designee.

2.2.9 “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 in regulations or other guidance issued under Section 13402(h)(2) of HITECH.

ARTICLE 3 OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

Business Associate agrees to:

3.1 Use and Disclosure. Not use or further disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.

3.2 Appropriate Safeguards. Use appropriate physical, technical, and administrative safeguards (a) to prevent use or disclosure of PHI other than as permitted under this Agreement or as Required By Law and (b) to reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

3.3 Assurances. Provide Covered Entity with written assurances that any PHI placed on any type of mobile media, including, but by no means limited to, lap top computers, Ipads and mobile phones, is encrypted in accordance with guidance issued by the Secretary.

3.4 Breach Reporting. Report in writing to Covered Entity within ten (10) business days after discovery, any suspected or actual: (a) access, use or disclosure of PHI not permitted by this Agreement; (b) breach of unsecured PHI in accordance with 45 CFR 164.410; (c) security breach or intrusion; (d) use or disclosure of PHI in violation of any applicable federal or state laws or regulations. Business Associate will implement a reasonable system for discovery of Breaches.

3.5 Mitigation. Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

3.6 Agents and Subcontractors. Ensure that any agent, including a subcontractor, that creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate agrees to the same restrictions, conditions and requirements that apply through this Agreement to Business Associate with respect to such information.

3.7 Access to PHI. In the event that the Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to provide access, within ten (10) days of a request by Covered Entity in the time and manner designated by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524.

3.8 Amendment of PHI. In the event that the Business Associate maintains Protected Health Information in a Designated Record Set, Business Associate agrees to make any

amendment(s) to Protected Health Information in a designated record set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, within ten (10) days of receipt of a request from Covered Entity and in the time and manner designated by Covered Entity.

3.9 Document Disclosures. Document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

3.10 Accounting of Disclosures. Within ten (10) days of notice by Covered Entity of a request for an accounting of disclosures of PHI, provide to Covered Entity, in the time and manner designated by Covered Entity, information collected in accordance with Section 3.9, 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 CFR 164.528.

3.11 Compliance with Applicable Requirements. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s).

3.12 Electronic Transactions. If Business Associate conducts any Standard Transaction for or on behalf of Covered Entity, Business Associate shall comply with the requirements under the Electronic Transaction Rule (as those terms are defined in the Security Rule).

3.13 Government Access. Make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule. In the event such a request comes directly from the Secretary, Business Associate agrees to notify Covered Entity immediately of such request.

3.14 Inspection. Within ten (10) business days of a written request by Covered Entity, Business Associate and its agents or subcontractors, if any, shall allow Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of PHI pursuant to this Agreement for the purpose of determining whether Business Associate has complied with this Agreement; provided, however, that (a) Business Associate and Covered Entity will mutually agree in advance upon the scope, location and timing of such an inspection, and (b) Covered Entity will protect the confidentiality of all confidential and proprietary information of Business Associate to which Covered Entity has access during the course of such inspection.

3.15 Identity Theft. Implementation of an Identity Theft Monitoring Policy and Procedure, to protect any patient information that may be breached by the Business Associate to the extent applicable under the Federal Trade Commission's Red Flag Rules.

3.16 HITECH Compliance. Business Associate shall:

3.16.1 not receive, directly or indirectly, any impermissible remuneration in exchange for PHI or ePHI, except as permitted by HITECH § 13405(d) or the HIPAA Regulations;

3.16.2 comply with the marketing and other restrictions applicable to business associates contained in HITECH § 13406 and the HIPAA Regulations;

3.16.3 to the extent required under HITECH § 13404, fully comply with the applicable requirements of 45 CFR 164.502(e)(2) for each use or disclosure of PHI;

3.16.4 to the extent required under HITECH § 13401, fully comply with 45 CFR 164.308, 164.310, 164.312, and 164.316;

3.16.5 to the extent required under HITECH §§ 13401 and 13404, comply with the additional privacy and security requirements that apply to covered entities in the same manner and to the same extent as Covered Entity is required to do so; and

3.16.6 to the extent required under the HIPAA Regulations, comply with the privacy and security requirements that apply to business associates.

3.17 State Privacy Laws. Business Associate shall understand and comply with state privacy laws to the extent that such state privacy laws are not preempted by HIPAA or HITECH. Without limiting the generality of the foregoing, all of Business Associate's uses and disclosures of PHI shall be consistent with: (a) the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code Section 56 *et seq.*; and (b) Cal. Health and Safety Code Section 1280.15.

ARTICLE 4 PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

Except as otherwise limited in this Agreement:

4.1 Business Associate may use or disclose Protected Health Information to perform functions, activities or services for, or on behalf of, Covered Entity, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

4.2 Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

ARTICLE 5 OBLIGATIONS OF COVERED ENTITY

5.1 Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

5.2 Permissible Requests. 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.

ARTICLE 6 TERM AND TERMINATION

6.1 Term. The obligations set forth in this Agreement shall be effective as of the date the first Protected Health Information is released to Business Associate pursuant to this Agreement, and shall terminate only 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 infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Article 6.

6.2 Termination for Cause. Upon Covered Entity's knowledge of a material breach 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 if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity.

6.3 Effect of Termination.

6.3.1 Except as provided in Section 6.3.2, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

6.3.2 In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

ARTICLE 7 MISCELLANEOUS

7.1 Indemnification. Business Associate agrees to indemnify, defend, and hold harmless Covered Entity, its directors, officers, employees, contractors and agents, against, and in respect of, any and all claims, losses, expenses, costs, damages, obligations, penalties, and liabilities which Covered Entity may incur by reason of Business Associate's breach of or failure to perform any of its obligations pursuant to this Agreement. Further, Business Associate agrees to indemnify, defend, and hold harmless Covered Entity, its directors, officers, employees, contractors and agents, against all costs and expenses, including but not limited to, reasonable legal expenses, which are incurred by or on behalf of Business Associate in connection with the defense of such claims.

7.2 Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with this Agreement, HIPAA, HITECH, or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

7.3 Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself, and any subcontractors, employees, affiliates or agents assisting Business Associate in the performance of its obligations under this Agreement, available to Covered Entity, at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, its directors, officers or employees based upon a claimed violation of HIPAA, HITECH, the HIPAA Regulations, or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee or agent is named adverse party.

7.4 Survival. The respective rights and obligations of Business Associate under this section shall survive the termination of this Agreement.

7.5 Ownership of Information. Covered Entity holds all right, title, and interest in and to the PHI and Business Associate does not hold and will not acquire by virtue of this Agreement or by virtue of providing goods or services to Covered Entity, any right, title, or interest in or to the PHI or any portion thereof.

7.6 Right to Injunctive Relief. Business Associate expressly acknowledges and agrees that the breach, or threatened breach, by it of any provision of this Agreement may cause Covered Entity to be irreparably harmed and that Covered Entity may not have an adequate remedy at law. Therefore, Business Associate agrees that upon such breach, or threatened breach, Covered Entity will be entitled to seek injunctive relief to prevent Business Associate from commencing or continuing any action constituting such breach without having to post a bond or other security and without having to prove the inadequacy of any other available remedies. Nothing in this paragraph will be deemed to limit or abridge any other remedy available to Covered Entity at law or in equity.

7.7 Regulatory References. A reference in this Agreement to a section in HIPAA, HITECH or the HIPAA Regulations means the section as in effect or as amended.

7.8 Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the HIPAA Regulations.

7.9 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Regulations.

7.10 Severability. In the event any part or parts of this Agreement are held to be unenforceable, the remainder of this Agreement will continue in effect.

(i) California HIPAA Rule. **Understand and Comply with California Senate Bill 541 and AB 211** to the extent applicable which requires health facilities, clinics, hospices and home health agencies to prevent unlawful or unauthorized access to, or use or disclosure of, a patient's medical information. This requirement creates a stricter standard than any currently in effect under existing state law or HIPAA because facilities are required under this bill to "prevent" unauthorized access, not merely to take reasonable steps to try to monitor and stop inappropriate access.

SB 541 also authorizes administrative penalties on the facility of up to \$25,000 per patient per violation, and up to \$17,500 for each subsequent accessing, use or disclosure of that information, and increases existing penalties for violations that result in immediate jeopardy of patients.

Assembly Bill 211 requires that every health care provider implement specified safeguards to protect the privacy of a patient's medical information, and establishes an Office of Health Information Integrity (OHII) within the California Health and Human Services Agency, which will assess and impose fines for violations of privacy laws. Penalties may be assessed: against any person or provider of health care, whether licensed or unlicensed up to \$250,000 as set forth in CMIA and requires referral from DPH for assessment of fines.

7.10 Notices. All notices, requests, demands, and other communications required or permitted under this BAA shall be in writing and shall be deemed to have been duly given, made, and received (a) when personally delivered, (b) on the day specified for delivery deposited with a courier service such as Federal Express for delivery to the intended addressee, or (c) three (3) business days following the day deposited in the United States mail, registered or certified mail, postage prepaid, return receipt requested, to the address as set forth below:

If to Business Associate:

If to Covered Entity:

Community Memorial Health System
Attn: Compliance Department
147 North Brent St.
Ventura, CA 93003
Tel No.: 805-652-4273

[SIGNATURES ON NEXT PAGE]

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the date first written above.

COMMUNITY MEMORIAL HEALTH SYSTEM:

Emilie Rayman, Chief Compliance Officer

Date: _____

BUSINESS ASSOCIATE:

By: _____

Name: _____

Title: _____

Date: _____