BUSINESS ASSOCIATE AGREEMENT HIPAA & HITECH

V: LVMC Business Associate Agreement 2023

THIS HIPAA Business Associate Agreement (the "**BA Agreement**") is entered into as of date _____ (the "**Effective Date**"), between Lompoc Valley Medical Center (the "**Client**") and _____ (the "**Company**"), in connection with (i) certain agreements or contracts between the Client and Company, and (ii) all related written agreements that the Parties may enter into in the future "**Service Agreement(s)**." The Client and the Company are hereinafter referred to collectively as the "**Parties**" and individually as a "**Party**."

WHEREAS, the Client is a "covered entity" as defined in 45 CFR Part 160.103;

WHEREAS, Company is a "business associate" as defined in 45 CFR Part 160.103;

WHEREAS, each Party may be provided with, have access to, create, view, disseminate "protected health information" ("PHI"), as defined in 45 CFR Part 160.103, relating to the Client's patients in connection with the Service Agreement(s);

WHEREAS, Client and Company intend to protect the privacy and provide for the protection of PHI in compliance with the **Health Insurance Portability and Accountability Act of 1996**, Public Law 104-101 ("**HIPAA**") and the regulations promulgated there under, including, without limitation, the regulations codified at 45 CFR Parts 160, 162 and 164 (the "**HIPAA Regulations**"), and other applicable laws, in each case, as amended from time to time (collectively the "**HIPAA Laws**") including the **Security Rule and Health Information Technology for Economic and Clinical Health (HITECH) Act**, enacted as part of the American Recovery and Reinvestment Act of 2009, signed into law on February 17, 2009; and

WHEREAS, the HIPAA Regulations require a business associate to enter into an agreement with a covered entity containing certain requirements with respect to the use and disclosure of PHI which are intended to be memorialized in this BA Agreement.

NOW, THEREFORE, in consideration of the mutual promises contained herein and the exchange of information pursuant to this BA Agreement, the Parties agree as follows:

1. Definitions.

   Capitalized terms used herein without definition shall have the meanings ascribed thereto in the Service Agreement(s) or the HIPAA Regulations whichever is applicable.

2. Obligations of Each Party with respect to PHI.

   a. Permitted Uses and Disclosures of Protected Health Information. Company May Use and Disclose PHI as necessary to perform the services under the Service Agreement(s). Company may not Use or further Disclose PHI in a manner that would violate the Privacy Regulations if done by the Client. Company may Use and Disclose PHI for the proper management and administration of the Company provided that such Disclosures are required by law, or the Company obtains reasonable assurances from the person to whom the information is Disclosed that it will remain confidential and will be 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 Company of any instances of which it is aware that the confidentiality of the information has been breached. If authorized as part of the services under the Service Agreement(s), Company may Use PHI to provide data aggregation services to Client. Data aggregation (or "Aggregated Data") means the combining of PHI created or received by the Company on behalf of Client with PHI received by the Company in its capacity as the business associate of another covered entity, to permit data analyses that relate to the health care operations of Client. Notwithstanding the foregoing, Company acknowledges it has no ownership right with respect to Client's PHI or Aggregated Data. To the extent that Company is

to carry out the Client's obligations under Subpart E of 45 C.F.R. Part 164, it shall comply with the requirements of such Subpart that apply to the Client in the performance of such obligations. Company Associate shall not Use or Disclose PHI for any other purpose.

b. Appropriate Safeguards. Each Party shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI, including ePHI, that Company creates, receives, maintains, uses or transmits on behalf of Client and to prevent Use or Disclosure of PHI other than as provided for by this Agreement. Company shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of Subpart C of 45 C.F.R. Part 164. Each Party shall maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size of and complexity of their operations and the nature and scope of its activities.

c. Duty to Mitigate. Each Party agrees to mitigate, to the extent practicable, any harmful effect that is known to such Party of a use or disclosure of PHI by such Party in violation of the requirements of this BA Agreement.

d. Reporting of Breach. The Company shall report to Client, by telephone and in writing, any Security Incident, Breach of Unsecured PHI, or unauthorized Use or Disclosure of PHI not permitted under the HIPAA regulations or by this BA Agreement ("**Breach**") within a reasonable time of becoming aware of such Breach (but no later than 12 hours thereafter), in accordance with the notice provisions set forth herein. Such notice shall be confirmed, within 48 hours, in writing via facsimile transmission. Company shall take (i) prompt action to cure any deficiencies in its systems that resulted in such Breach; and (ii) any action pertaining to such Security Breach required by the HIPAA Regulations. Company shall take all actions necessary to enable the Client to notify individuals and the Secretary of any Breach to the extent required by the HIPAA Regulations.

e. Identity Theft. In the event that Company is engaged to perform any "creditor" related activity in connection with any of the Client's "covered accounts" (as defined in 16 C.F.R. § 681.2(d)(2), *et seq*., and commonly referred to as the "**Red Flag Rules**"; see, also 72 F.R. 63727), Company agrees to fully adopt and comply with the Red Flag Rules, which require, among other things, identification of factors that suggest risk of identity theft, and the adoption of an Identity Theft Prevention Program that is compliant with applicable federal regulations, and to conduct its activities in accordance with reasonable policies and procedures to detect, prevent, and mitigate the risk of identity theft.

f. Access to PHI. Within 10 days of receipt of a request, Company shall make PHI maintained in its database available to the Client or, as directed by the Client, to an individual to enable the Client to fulfill its obligations under Section 164.524 of the HIPAA Regulations. Company agrees that it will disclose PHI as needed by Client to satisfy its obligations to respond to an individual's request for an electronic copy of his/her PHI. In the event that any individual requests access to PHI directly from Company, Company shall forward such request to the Client. A denial of access to requested PHI shall not be made without the prior written consent of the Client.

As of the Effective Date of this Agreement, Company obligations described above will include additional safeguards required to be taken by Company pursuant to such Section 13401(a). Notwithstanding the foregoing, when Company is present at a facility of Client or its affiliates or is accessing or utilizing a system owned, leased or licensed by Client or its affiliates ("Client Systems"), Company will comply with Client's standard safeguards to prevent the use or disclosure of PHI (including Client's standard administrative, physical and technical safeguards to protect the

confidentiality, integrity, and availability of Electronic PHI) applicable to such Client facility or such Client System, provided Client has given Company prior notice of such safeguards in writing or in the same manner as Client provides notice of such safeguards to its own employees and other contractors.

Except as provided in Section 13405(d)(2) of the HITECH Act, Company will not directly or indirectly receive remuneration in exchange for any PHI of an Individual unless Client has obtained from the Individual, in accordance with 45 C.F.R. & 164.508, a valid authorization that includes, in accordance with such section, a specification of whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that Individual.

g. Amendment of PHI. Company shall amend/revise the PHI it maintains in a Designated Record Set as requested by the Client within 10 days of receipt of such request to enable the Client to fulfill its obligations under Section 164.526 of the HIPAA Regulations. If any individual requests an amendment of its PHI directly from Company, Company must notify the Client in writing within five days of the request. Company shall not deny a request to amend PHI from the individual or the without the prior written consent of the Client.

h. Accounting of Disclosures of PHI. Company shall make available to the Client the information required to provide an accounting of disclosures of PHI to enable the Client to fulfill its obligations under Section 164.528 of the HIPAA Regulations. Company agrees to maintain a process that allows for an accounting of disclosures of PHI to be collected and provided to the Client in accordance with this subsection. Further, Company agrees that upon termination or expiration of the Service Agreement(s), Company shall provide to the Client an accounting of all such disclosures made during the existence of the Service Agreement(s). At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to Company, Company shall, within five days of a request, forward it to the Client in writing. It shall be Company's responsibility to prepare, and the Client's responsibility to deliver to the individual, any such accounting requested.

i. Governmental Access to Records. Upon reasonable request, Company shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services (the "**Secretary**") for purposes of determining the Business's compliance with the HIPAA Regulations. Notwithstanding the foregoing, no attorney-client, accountant-client or other legal privilege shall be deemed waived by Company or the Client by virtue of this section. Except to the extent prohibited by the HIPAA Regulations, each Party agrees to notify the other Party of all applicable requests served upon such Party for information or documents by or on behalf of the Secretary.

j. Minimum Necessary. A Party shall only request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure.

k. Company Insurance. Company shall obtain and maintain, during the term of the this BA Agreement, reasonable liability insurance covering claims based on any violation by Company of the terms of this BA Agreement, if such insurance is reasonably available. A copy of such policy or a certificate evidencing such policy shall be provided to the Client upon request.

l. Audits, Inspection and Enforcement. Within 10 days of a written request by the Client, Company shall allow the Client 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 BA Agreement for the purpose of determining whether Company has complied with this BA Agreement; provided, however, that (i) Company shall agree in advance upon the scope, timing and location of such an inspection; (ii) the Client shall protect the confidentiality of all confidential and proprietary information of Company to which it has access during the course of such inspection; and (iii) the Client shall execute a nondisclosure agreement upon terms mutually agreed upon by the Parties, if requested by Company. The fact that the Client inspects, or fails to inspect, or has the right to inspect, Company's facilities, systems, books, records, agreements, policies and procedures does not relieve Company of its responsibility to comply with this BA Agreement, nor does the Client's (i) failure to detect or (ii) detection, but failure to notify Company or require Company's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of the Client's enforcement rights under this BA Agreement.

m. State Privacy Laws. Each Party shall comply with California State privacy laws to the extent that such state privacy laws are not preempted by HIPAA.

3. Termination.

a. Breach. A material breach or violation by Company of any provision of this BA Agreement, as determined in good faith by the Client, shall constitute a breach of this BA Agreement and shall provide grounds for immediate termination of the Service Agreement(s) by the Client.

As required by Section 13404(b) of the HITECH Act, if Company commits a material breach of its obligations in this Agreement, Client may (a) terminate this Agreement by providing Client prior written notice if Company fails to cure such breach within thirty (30) days of its receipt of written notice from Client specifying the nature of such breach; (b) immediately terminate this Agreement by providing Client prior written notice if a cure of such breach is not possible.

b. Judicial or Administrative Proceedings. The Client may terminate the Service Agreement(s), effective immediately, if (i) Company is named as a defendant in a criminal proceeding for an offense related to healthcare or (ii) a finding or stipulation that Company has violated any standard or requirement of any law or regulation relating to healthcare is made in any administrative or civil proceeding in which Company has been joined.

c. Effect of Termination. Upon termination of this BA Agreement for any reason, the Client shall either return or destroy all PHI, as requested by the Client and shall retain no copies of such PHI. If the Client requests that Company return PHI, such PHI shall be returned in a mutually agreed upon format and timeframe, at no additional charge to the Client. If return or destruction is not feasible, Company shall continue to extend the protections of this BA Agreement to such information, and limit further uses and disclosures of such PHI to those purposes that make the return or destruction of such PHI not feasible. If Company is to destroy the PHI, Company shall certify in writing to the Client that such PHI has been destroyed.

4. Use of Subcontractors and Agents: Company shall require each of its agents and subcontractors that create, receive, maintain, or transmit PHI from Company on behalf of Client, to execute a written agreement obligating the agent or subcontractor to comply with the same restrictions and conditions that apply to Company under this Agreement including, without limitation, implementation of reasonable and appropriate administrative,

physical and technical safeguards to protect such PHI and ePHI and requirements that Security Incidents and Breaches of Unsecured PHI be reported to the Client.

5. Indemnification. Company will immediately indemnify and pay Client for and hold it harmless from (i) any and all fees and expenses Client incurs in investigating, responding to, and/or mitigating a breach of PHI or confidential data caused by Company or its subcontractors or agents; (ii) any damages, attorneys' fees, costs, liabilities or other sums actually incurred by Plan due to a claim, lawsuit, or demand by a third party arising out of a breach of PHI or confidential data caused by Company or its subcontractors or agents; and/or (iii) for fines, assessments and/or civil penalties assessed or imposed against Client by any government agency/regulator based on a breach of PHI or confidential data caused by Company or its subcontractors or agents. Such fees and expenses may include, without limitation, attorneys' fees and costs and costs for computer security consultants, credit reporting agency services, postal or other delivery charges. Acceptance by Client of any insurance certificates and endorsements required under the [Agreements] does not relieve Company from liability under this indemnification provision. This provision shall apply to any damages or claims for damages whether or not such insurance policies shall have been determined to apply.

6. Disclaimer. A Party makes no warranty or representation that compliance by the other Party with this BA Agreement, HIPAA or the HIPAA Regulations will be adequate or satisfactory for such Party's own purposes. Each Party is solely responsible for all decisions made by it regarding its safeguarding of PHI.

7. Certification. To the extent that the Client determines in good faith it is necessary in order to comply with its legal obligations relating to certification under HIPAA of its security practices, the Client may require Company to certify its compliance with the security provisions of HIPAA, or, at the Client's expense, examine Company facilities, systems, procedures and records as may be necessary to issue such certification.

8. Amendment. The Parties acknowledge that state and federal laws relating to PHI security and patient privacy are rapidly evolving and that an amendment of this BA Agreement may be required to provide for procedures to ensure compliance with such developments. The Parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HIPAA Regulations and other applicable laws relating to the security or confidentiality of PHI. The Parties understand and agree that the Client must receive satisfactory written assurance from Company that Company will adequately safeguard all PHI. Upon the request of the Client, Company agrees to promptly enter into negotiations concerning the terms of an amendment to this BA Agreement embodying written assurances consistent with the standards and requirements of HIPAA, the HIPAA Regulations or other applicable laws. The Client may terminate the BA Agreements upon 30 days written notice in the event (i) Company does not promptly enter into negotiations to amend this BA Agreement when requested by the Client pursuant to this Section 7 or (ii) Company does not enter into an amendment to this BA Agreement providing assurances regarding the safeguarding of PHI that the Client in good faith deems necessary to satisfy the standards and requirements of HIPAA and the HIPAA Regulations.

9. Assistance in Litigation or Administrative Proceedings. Each Party shall make itself, and its employees or agents assisting it in the performance of its obligations under this BA Agreement, available to the other Party at no cost to such Party, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against such Party, its directors, officers or employees based upon a claimed violation of HIPAA, the HIPAA Regulations or other laws relating to security and privacy, except where a Party or its employee or agent is a named adverse party.

10. No Third Party Beneficiaries. Nothing express or implied in this BA Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and

their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

11. Effect on the Service Agreement(s). Except to the extent inconsistent with this BA Agreement, all other terms of the Service Agreement(s) shall remain in force and effect.

12. Survival. The provisions of this BA Agreement shall survive the termination or expiration of the Service Agreement(s).

13. Interpretation. The provisions of this BA Agreement shall prevail over any provisions in the Service Agreement(s) that may conflict or appear inconsistent with any provision in this BA Agreement. This BA Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and the HIPAA Regulations. The Parties agree that any ambiguity in this BA Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA Regulations.

14. Governing Law. This BA Agreement shall be construed in accordance with the laws of the United States of America and the State of California when applicable.

15. Notices. All notices required or permitted under this BA Agreement shall be in writing and sent to the other Party as directed by such Party, from time to time, by written notice to the other.

16. Facsimile and Counterparts. This BA Agreement may be signed by facsimile and executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument

IN WITNESS WHEREOF, the Parties hereto have duly executed this BA Agreement as of the Effective Date.

THE CLIENT, Lompoc Valley Medical Center
1515 East Ocean Avenue
Lompoc, California 93436

THE COMPANY, _____

Signature: _____

Name: _____

Title: _____

Signature: _____

Name: _____

Title: _____