

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“BAA”) effective June 1, 2022 (“Effective Date”), is entered into by and among between the County of Monterey, a political subdivision of the State of California, on behalf of Natividad Medical Center (“Covered Entity”) and CareFusion Solutions, LLC, together with its affiliates (“Business Associate”) (each a “Party” and collectively the “Parties”).

RECITALS

A. WHEREAS, Business Associate provides certain Services for Covered Entity that involve the Use and Disclosure of Protected Health Information (“PHI”) that is created, received, transmitted, or maintained by Business Associate for or on behalf of Covered Entity.

B. WHEREAS, The Parties are committed to complying with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), and their implementing regulations, including the Standards for the Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E (the “Privacy Rule”), the Breach Notification Standards, 45 C.F.R. Part 160 and 164 subparts A and D (the “Breach Notification Rule”), and the Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C (the “Security Rule”), (collectively “HIPAA”), all as amended from time to time.

C. WHEREAS, The Parties are also committed to complying with the California Confidentiality Laws (defined below) where applicable and not preempted by HIPAA or the HITECH Act.

D. WHEREAS, To the extent that Business Associate is performing activities in connection with covered accounts for or on behalf of Covered Entity, the Parties are also committed to complying with applicable requirements of the Red Flag Rules issued pursuant to the Fair and Accurate Credit Transactions Act of 2003 (“Red Flag Rules”).

E. WHEREAS, The Privacy and Security Rules require Covered Entity and Business Associate to enter into a business associate agreement that meets certain requirements with respect to the Use and Disclosure of PHI. This BAA, sets forth the terms and conditions pursuant to which PHI, and, when applicable, Electronic Protected Health Information (“EPHI”) shall be handled, in accordance with such requirement.

F. WHEREAS, this Agreement shall apply only to the extent that Business Associate receives PHI and is considered a Business Associate in its performance of the Services according to the meaning set forth in 45 C.F.R. § 160.103.

NOW THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this BAA, the Parties agree as follows:

AGREEMENT

1. DEFINITIONS

1.1 All capitalized terms used in this BAA but not otherwise defined shall have the meaning set forth in the Privacy Rule, the Breach Notification Rule, or the Security Rule.

(a) “Breach” shall have the same meaning as “breach” as defined in 45 C.F.R. § 164.402 and shall mean the access, acquisition, Use, or Disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the privacy or security of the PHI; the term “Breach” as used in this BAA shall also mean the unlawful

or unauthorized access to, Use or Disclosure of a patient’s “medical information” as defined under Cal. Civil Code § 56.05(j), for which notification is required pursuant to Cal. Health & Safety Code 1280.15, or a “breach of the security of the system” under Cal. Civil Code §1798.29.

(b) “California Confidentiality Laws” shall mean the applicable laws of the State of California governing the confidentiality of PHI or Personal Information, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq.), the patient access law (Cal. Health & Safety Code §123100 et seq.), the HIV test result confidentiality law (Cal. Health & Safety Code §120975, et seq.), the Lanterman-Petris-Short Act (Cal. Welf. & Inst. Code §5328, et seq.), and the medical identity theft law (Cal. Civil Code 1798.29).

(c) “Protected Health Information” or “PHI” shall mean any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual; (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information that can be used to identify the individuals, and (iii) is provided by Covered Entity to Business Associate or created, maintained, received, or transmitted by Business Associate on Covered Entity’s behalf. **PHI includes EPHI.**

(d) “Services” shall mean the services for or functions on behalf of Covered Entity performed by Business Associate pursuant to a Services Agreement between Covered Entity and Business Associate to which this BAA applies.

2. PERMITTED USES AND DISCLOSURES OF PHI

Unless otherwise limited herein, Business Associate may:

(a) Use or Disclose PHI to perform Services for, or on behalf of, Covered Entity, provided that such Use or Disclosure would not violate the Privacy or Security Rules, this BAA, or California Confidentiality Laws;

(b) Use or Disclose PHI for the purposes authorized by this BAA or as otherwise Required by Law;

(c) Use PHI to provide Data Aggregation Services for the Health Care Operations of Covered Entity, if required by the Services Agreement and as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B);

(d) Use PHI if necessary for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate as permitted by 45 C.F.R. § 164.504(e)(4)(i);

(e) Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate as permitted under 45 C.F.R. § 164.504(e)(4)(ii), 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 be Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and that such person will notify the Business Associate of any instances of which such person is aware that the confidentiality of the information has been breached;

(f) Use PHI to report violations of law to appropriate Federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1); and

(g) De-identify any PHI obtained by Business Associate under this BAA in accordance with 45 C.F.R. § 164.514 and Use or Disclose such de-identified information only as required to provide Services pursuant to the Services Agreement between the Parties, or with the prior written approval of Covered Entity.

3. RESPONSIBILITIES OF THE PARTIES WITH RESPECT TO PHI

3.1. Responsibilities of Business Associate. With regard to its Use and/or Disclosure of PHI, Business Associate shall:

(a) Notify the Privacy Officer of Covered Entity, in writing, of: (i) any Use and/or Disclosure of the PHI that is not permitted or required by this BAA; (ii) any Security Incident of which Business Associate becomes aware; and (iii) any Breach. Such notice shall be provided within five (5) business days of Business Associate's discovery of such unauthorized access, acquisition, Use and/or Disclosure. Notwithstanding the foregoing, the Parties acknowledge the ongoing existence and occurrence of attempted but ineffective Security Incidents that are trivial in nature, such as pings and other broadcast service attacks, and unsuccessful log-in attempts. The Parties acknowledge and agree that this Section 3.1(a) constitutes notice by Business Associate to Covered Entity of such ineffective Security Incidents and no additional notification to Covered Entity of such ineffective Security Incidents is required, provided that no such Security Incident results in a Breach. A ransomware attack that involves, or that can be reasonably expected to involve, Covered Entity PHI shall not be considered an ineffective Security Incident and shall be reported to Covered Entity, irrespective of whether such Security Incident results in a Breach. Business Associate shall investigate each Security Incident or unauthorized access, acquisition, Use, or Disclosure of PHI, or Breach that it discovers and shall provide a summary of its investigation to Covered Entity, upon request. If Business Associate or Covered Entity determines that such Security Incident or unauthorized access, acquisition, Use, or Disclosure, or Breach constitutes a Breach, then Business Associate shall comply with the requirements of Section 3.1(a)(i) below;

(i) Business Associate shall provide a supplemental written report in accordance with 45 C.F.R. § 164.410(c), which shall include, to the extent possible, the identification of each individual whose PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, Used or Disclosed during the Breach, to Covered Entity without unreasonable delay, but no later than five (5) business days after discovery of the Breach;

(ii) Covered Entity shall have sole control over the timing and method of providing notification of such Breach to the affected individual(s), the appropriate government agencies, and, if applicable, the media. Business Associate shall reasonably assist with the implementation of any decisions by Covered Entity to notify individuals or potentially impacted individuals, upon Covered Entity's reasonable written request;

(b) In consultation with the Covered Entity, Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of such improper access, acquisition, Use, or Disclosure, Security Incident, or Breach. Business Associate shall take prompt corrective action, including any action required by applicable State or federal laws and regulations relating to such Security Incident or non-permitted access, acquisition, Use, or Disclosure. Solely to the extent directly caused by Business Associate, Business Associate shall reimburse Covered Entity for its reasonable and actual costs and expenses in providing legally required notification to affected individuals, appropriate government agencies, and, if necessary the media, including, but not limited to, any administrative costs associated with providing notice, printing and mailing costs, public relations costs, attorney fees, and costs of mitigating the harm (which may include the costs of obtaining up to one year of credit monitoring services and identity theft insurance if there is a reasonable risk of identity theft) for affected individuals whose PHI or Personal Information has been compromised as a result of the Breach;

(c) Implement appropriate administrative, physical, and technical safeguards and comply with the Security Rule to prevent Use and/or Disclosure of EPHI other than as provided for by this BAA;

(d) Obtain and maintain a written agreement with each of its Subcontractors that creates, maintains, receives, Uses, transmits or has access to PHI that requires such Subcontractors to adhere to the substantially the same restrictions and conditions with respect to PHI that apply to Business Associate pursuant to this BAA;

(e) Make available all internal practices, records, books, agreements, policies and procedures and PHI relating to the Use and/or Disclosure of PHI received from, created, maintained, or transmitted by Business Associate on behalf of Covered Entity to the Secretary of the Department of Health and Human Services (“Secretary”) in a time and manner designated by the Secretary for purposes of determining Covered Entity’s or Business Associate’s compliance with the Privacy Rule. ;

(f) Document Disclosures of PHI and information related to such Disclosure and, within thirty (30) days of receiving a written request from Covered Entity, provide to Covered Entity such information as is requested by Covered Entity to permit Covered Entity to respond to a request by an individual for an accounting of the Disclosures of the individual’s PHI in accordance with 45 C.F.R. § 164.528. At a minimum, the Business Associate shall provide the Covered Entity with the following information: (i) the date of the Disclosure; (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person; (iii) a brief description of the PHI Disclosed; and (iv) a brief statement of the purpose of such Disclosure which includes an explanation of the basis for such Disclosure. In the event the request for an accounting is delivered directly to the Business Associate, the Business Associate shall, within ten (10) days, forward such request to the Covered Entity. The Business Associate shall implement an appropriate recordkeeping process to enable it to comply with the requirements of this Section;

(g) Subject to Section 4.4 below, return to Covered Entity within thirty (30) days of the termination of this BAA, the PHI in its possession and retain no copies, including backup copies;

(h) Disclose to its Subcontractors or other third parties, and request from Covered Entity, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder;

(i) If all or any portion of the PHI is maintained in a Designated Record Set:

(i) Upon ten (10) days’ prior written request from Covered Entity, provide access to the PHI to Covered Entity to meet a request by an individual under 45 C.F.R. § 164.524. Business Associate shall notify Covered Entity within ten (10) days of its receipt of a request for access to PHI from an Individual; and

(ii) Upon ten (10) days’ prior written request from Covered Entity, make any amendment(s) to the PHI that Covered Entity directs pursuant to 45 C.F.R. § 164.526. Business Associate shall notify Covered Entity within ten (10) days of its receipt of a request for amendment of PHI from an Individual;

(j) If applicable, maintain policies and procedures to detect and prevent identity theft in connection with the provision of the Services, to the extent required to comply with the Red Flag Rules;

(k) To the extent that Business Associate carries out one or more of Covered Entity’s obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligations;

(l) Unless prohibited by law, notify the Covered Entity within five (5) days of the Business Associate’s receipt of any request or subpoena for PHI. To the extent that the Covered Entity decides to assume responsibility for challenging the validity of such request, the Business Associate shall reasonably cooperate with the Covered Entity in such challenge; and

(m) Maintain policies and procedures materially in accordance with State Confidentiality Laws and industry standards designed to ensure the security and integrity of the Covered Entity's data and protect against threats or hazards to such security;

(n) Once annually and upon Covered Entity's reasonable written request, Business Associate agrees to provide a confidential summary of an audit performed by a qualified third party selected by Business Associate, such as a SOC 2.

3.2 Business Associate Acknowledgment.

(a) Business Associate acknowledges that, as between the Business Associate and the Covered Entity, all PHI shall be and remain the sole property of the Covered Entity.

(b) Business Associate further acknowledges that it is obligated by law to comply, and acknowledges and agrees that it shall comply, with HIPAA and the HITECH Act. Business Associate shall comply with all California Confidentiality Laws, to the extent that such state laws are not preempted by HIPAA or the HITECH Act.

(c) Business Associate further acknowledges that uses and disclosures of protected health information shall, to the extent commercially reasonable, be consistent with NMC's Notice of Privacy Practices attached hereto as Attachment A.

3.3 Responsibilities of Covered Entity. Covered Entity shall, with respect to Business Associate:

(a) Provide Business Associate a copy of Covered Entity's notice of privacy practices ("Notice") currently in use;

(b) Notify Business Associate of any changes to the Notice that Covered Entity provides to individuals pursuant to 45 C.F.R. § 164.520, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI;

(c) Notify Business Associate of any changes in, or withdrawal of, the consent or authorization of an individual regarding the Use or Disclosure of PHI provided to Covered Entity pursuant to 45 C.F.R. § 164.506 or § 164.508, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI; and

(d) Notify Business Associate of any restrictions on Use and/or Disclosure of PHI as provided for in 45 C.F.R. § 164.522 agreed to by Covered Entity, to the extent that such restriction may affect Business Associate's Use or Disclosure of PHI.

4. TERM AND TERMINATION

4.1 Term. This BAA shall become effective on the Effective Date and shall continue in effect unless terminated as provided in this Section 4. Certain provisions and requirements of this BAA shall survive its expiration or other termination as set forth in Section 5 herein.

4.2 Termination. If Covered Entity determines in good faith that Business Associate has breached a material term of this BAA, Covered Entity may either: (i) immediately terminate this BAA and the applicable underlying Services Agreement that granted access to the data that gave rise to the breach; or (ii) terminate this BAA and the applicable underlying Services Agreement that granted access to the data that gave rise to the breach within sixty (60) days of Business Associate's receipt of written notice of such breach, if the breach is not cured to the reasonable satisfaction of Covered Entity.

4.3 Automatic Termination. This BAA shall automatically terminate without any further action of the Parties upon the termination or expiration of Business Associate’s provision of Services to Covered Entity.

4.4 Effect of Termination. Upon termination or expiration of this BAA for any reason, Business Associate shall return all PHI pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(J) if, and to the extent that, it is feasible to do so. Prior to returning the PHI, Business Associate shall recover any PHI in the possession of its Subcontractors. To the extent it is not feasible for Business Associate to return or destroy any portion of the PHI, Business Associate shall provide Covered Entity with a statement that Business Associate has determined that it is infeasible to return or destroy all or some portion of the PHI in its possession or in possession of its Subcontractors. In such event, Business Associate shall: (i) retain only that PHI which is necessary for Business Associate to continue its proper management and administration or carry out its legal responsibilities; (ii) return to Covered Entity or destroy the remaining PHI that the Business Associate maintains in any form; (iii) continue to extend the protections of this BAA to the PHI for as long as Business Associate retains PHI; (iv) limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction of the PHI not feasible and subject to the same conditions as set out in Section 2 above, which applied prior to termination; and (v) return to Covered Entity or destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

5. MISCELLANEOUS

5.1 Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 2.1, 4.4, 5.7, 5.8, 5.11, and 5.12 shall survive termination of this BAA until such time as the PHI is returned to Covered Entity or destroyed. In addition, Section 3.1(i) shall survive termination of this BAA, provided that Covered Entity determines that the PHI being retained pursuant to Section 4.4 constitutes a Designated Record Set.

5.2 Amendments; Waiver. This BAA may not be modified or amended, except in a writing duly signed by authorized representatives of the Parties. To the extent that any relevant provision of HIPAA, the HITECH Act, or California Confidentiality Laws is materially amended in a manner that changes the obligations of the Parties, the Parties agree to negotiate in good faith appropriate amendment(s) to this BAA to give effect to the revised obligations. Further, no provision of this BAA shall be waived, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

5.3 No Third-Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

5.4 Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party’s address given below, and/or via facsimile to the facsimile telephone numbers listed below.

If to Business Associate, to:

CareFusion Solutions, LLC
Attn: Legal Dept/BAA Compliance
3750 Torrey View Ct
San Diego, CA 92130
Phone:
E-Mail:

GMB-US-BAA-Legal@bd.com

If to Covered Entity, to:

Natividad Medical Center
Attn: Compliance/Privacy Officer

1441 Constitution Blvd.
Salinas, CA 93906
Phone: 831-755-4111
Fax: 831-755-6254

Each Party named above may change its address and that of its representative for notice by the giving of notice thereof in the manner hereinabove provided. Such notice is effective upon receipt of notice, but receipt is deemed to occur on next business day if notice is sent by FedEx or other overnight delivery service.

5.5 Counterparts; Facsimiles. This BAA may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

5.6 Relationship of Parties. Notwithstanding anything to the contrary in the Services Agreement, Business Associate is an independent contractor and not an agent of Covered Entity under this BAA. Business Associate has the sole right and obligation to supervise, manage, contract, direct, procure, perform, or cause to be performed all Business Associate obligations under this BAA.

5.7 Choice of Law; Interpretation. This BAA shall be governed by the laws of the State of California. Any ambiguities in this BAA shall be resolved in a manner that allows Covered Entity and Business Associate to comply with the Privacy Rule, the Security Rule, and the California Confidentiality Laws.

5.8 Indemnification. Business Associate shall indemnify, defend, and hold harmless the County of Monterey (the "County"), its officers, agents, and employees from any third party-claim for an actual liability, loss, injury, cost, expense, penalty or damage, including costs incurred by the County with respect to any investigation, enforcement proceeding, or third party action, (collectively "Costs") solely to the extent such Costs are directly arising out of a violation of this BAA or a Breach that is attributable to an act or omission of Business Associate and/or its agents, members, employees, or Subcontractors, excepting only loss, injury, cost, expense, penalty or damage caused by the negligence or willful misconduct of personnel employed by the County. This provision is in addition to, and independent of, any indemnification provision in any related or other agreement between the Parties.

5.9 Applicability of Terms. This BAA applies to all present and future Service Agreements and Business Associate relationships, written or unwritten, formal or informal, in which Business Associate creates, receives, transmits, or maintains any PHI for or on behalf of Covered Entity in any form whatsoever. This BAA shall automatically be incorporated in all subsequent agreements between Business Associate and Covered Entity involving the Use or Disclosure of PHI whether or not specifically referenced therein. In the event of any conflict or inconsistency between a provision of this BAA and a provision of any other agreement between Business Associate and Covered Entity with respect to the subject matter of this BAA, the provision of this BAA shall control.

5.10 Insurance. In addition to any general and/or professional liability insurance required of Business Associate, Business Associate agrees to obtain and maintain, at its sole expense, liability insurance on a claims made basis, covering any and all claims, liabilities, demands, damages, losses, costs and expenses arising from a breach of the obligations of Business Associate, its officers, employees, agents and Subcontractors under this BAA. Such insurance coverage will be maintained for the term of this BAA, and Memorandum of Insurance shall be provided to Covered Entity at Covered Entity's request. The Parties agree that Business Associate may self-insure for all or any portion of the required insurance.

5.11 Legal Actions. Promptly, but no later than five (5) business days after notice thereof, Business Associate shall advise Covered Entity of any actual action, proceeding, regulatory or governmental orders or actions, or any material threat thereof that becomes known to it that involves Covered Entity's PHI or jeopardize this BAA, and of any facts and circumstances that may be pertinent to the prosecution or defense of any such actual legal action or proceeding, except to the extent prohibited by law.


5.12 Audit or Investigations. Promptly, but no later than five (5) calendar days after notice thereof, Business Associate shall advise Covered Entity of any audit, compliant review, or complaint investigation by the Secretary or other state or federal agency related to compliance with HIPAA, the HITECH Act, or the California Confidentiality Laws involving Covered Entity PHI.

IN WITNESS WHEREOF, each of the undersigned has caused this BAA to be duly executed in its name and on its behalf as of the Effective Date.

BUSINESS ASSOCIATE

COVERED ENTITY

By:  _____
Print Name Nnaemeka Oguguo
Print Title Contract Analyst- MMS Dispensing
Date: 01-Jun-2022

By:  for Charles Harris, CEO
Print Name: Kristin Aldrich
Print Title: Deputy Purchasing Agent
Date: 6-1-22

NOTICE OF PRIVACY PRACTICES

Effective Date: April 14, 2003 | Revised Date: August 2016

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully. If you have any questions about this notice, please contact the Natividad Compliance Officer by calling the main Natividad number.

1. Who Will Follow This Notice

This notice describes Natividad's practices and that of:

- Health Care professionals authorized to enter information into your medical record at Natividad that have agreed to abide by this notice;
- all departments and units at Natividad;
- any member of a volunteer group we allow to help you while you are at Natividad;
- all employees, staff and other contract personnel that have agreed to abide by this notice, that use your health information to provide services to you at Natividad; and
- all Natividad Clinics

All these entities, and health care delivery sites, follow the terms of this notice. In addition, these entities, and health care delivery sites may share medical information with each other for treatment, payment or health care operations purposes described in this notice.

2. Our Pledge Regarding Medical Information

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We create a record of the care and services you receive at Natividad. We need this record to provide you with quality care and to comply with certain legal requirements. This notice applies to all of the records of your care generated by Natividad, whether made by Natividad personnel or your personal doctor. Your personal doctor may have different policies or notices regarding the doctor's use and disclosure of your medical information created in the doctor's office or clinic.

This notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information.

We are required by law to:

- make sure that medical information that identifies you is kept private (with certain exceptions);
- give you this notice of our legal duties and privacy practices with respect to medical information about you; and
- follow the terms of the notice that is currently in effect

3. How We May Use and Disclose Information About You

The following actions describe different ways that we use and disclose medical information. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

a. Disclosure at Your Request

We may disclose information when requested by you. This disclosure at your request may require a written authorization by you.

b. For Treatment

We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, nurses, technicians, medical students, or other Natividad personnel who are involved in taking care of you at Natividad. For example, a doctor treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process. In addition, the doctor may need to tell the dietitian if you have diabetes so that we can arrange for appropriate meals. Different departments or clinics at Natividad also may share medical information about you in order to coordinate the different things you need, such as prescriptions, lab work and x-rays. We also may disclose medical information about you to people outside Natividad who may be involved in your medical care after you leave Natividad.

c. What is Central Coast Health Connect (CCHC)?

CCHC is a community health information exchange (HIE), a system established to help patients and healthcare providers securely share health information electronically. An HIE helps to ensure that only you and the caregivers you authorize — including doctors, hospitals, and labs — have secure, instant access to vital medical information necessary to provide you the best care possible.

d. CCHC Health Information Exchange (HIE) at Natividad

The CCHC-HIE is a way of sharing personal health information among participating doctors' offices, hospitals, labs, radiology centers, and other healthcare providers through secure, electronic means. This gives participating providers the most recent information available from your other providers when they are making decisions about your care. Your information will be shared with the HIE unless you opt out.

e. What if I don't want to participate in CCHC?

If you don't want to participate in CCHC, you may choose to opt out. It is also important to understand that opting out prevents the sharing of your information through CCHC between providers. If they choose, your doctor and other care providers

will still be able to individually use the electronic health information exchange to have your lab results, radiology reports, and other data sent directly to them. Previously, they may have received this information by fax, mail, or other electronic communication. If you still choose to opt out, please email: cchc-help@centralcoasthealthconnect.org or call (831) 644-7494.

f. Maternity Patients

If you deliver an infant(s) while a patient of this hospital, we may use the same Notice of Privacy Practices for the infant(s).

g. For Payment

We may use and disclose medical information about you so that the treatment and services you receive at Natividad may be billed to and payment may be collected from you, an insurance company or a third party. For example, we may need to give your health plan information about surgery you received at Natividad so your health plan will pay us or reimburse you for the surgery. We may also tell your health plan about a treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment.

h. For Health Care Operations

We may use and disclose medical information about you for health care operations. These uses and disclosures are necessary to run Natividad and make sure that all of our patients receive quality care. For example, we may use medical information

to review our treatment and services, and to evaluate the performance of our staff in caring for you. We may also combine medical information about many Natividad patients to decide what additional services Natividad should offer, what services are not needed, and whether certain new treatments are effective. We may also disclose information to doctors, nurses, technicians, medical students, and other healthcare personnel for review and learning purposes. We may also combine the medical information we have with medical information from other healthcare institutions to compare how we are doing and see where we can make improvements in the care and services we offer. We may remove information that identifies you from this set of medical information so others may use it to study health care and health care delivery without learning who the specific patients are.

i. Appointment Reminders

We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment or medical care at Natividad or one of its clinics.

j. Treatment Alternatives

We may use and disclose medical information to tell you about or recommend possible treatment options or alternatives that may be of interest to you.

k. Health-Related Products and Services

We may use and disclose medical information to tell you about our health related products or services that may be of interest to you.

l. Fundraising Activities

We may use medical information about you to contact you in an effort to raise money for Natividad and its operations. We may disclose limited health information to Natividad Foundation so that the foundation may contact you in raising money for Natividad. We only would release contact information, such as your name, address and phone number and the dates you received treatment or services at Natividad. If you do not want the Natividad Foundation to contact you for fundraising efforts, you must notify the Foundation in writing.

m. Natividad Directory

We may include certain limited information about you in a facility directory while you are a patient at Natividad. This information may include your name, location in Natividad, your general condition (e.g., fair, stable, etc.) and your religious affiliation. Unless there is a specific written request from you to the contrary, this directory information, except for your religious affiliation, may also be released to people who ask for you by name. Your religious affiliation may be given to a member of the clergy, such as a priest or rabbi, even if they don't ask for you by name. This information is released so your family, friends and clergy can visit you at Natividad and generally know how you are doing.

n. Individuals Involved in Your Care or Payment for Your Care

We may release medical information about you to a friend or family member who is involved in your medical care. We may also release information to someone who helps pay for your care. Unless there is a specific written request from you to the contrary, we may also tell your family or friends your condition and that you are at Natividad. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location. If you arrive at the emergency department unconscious or otherwise unable to communicate,

we are required to attempt to contact someone we believe can make health care decisions for you (e.g., a family member or agent under a health care power of attorney).

o. Research

Under certain circumstances, we may use and disclose medical information about you for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another, for the same condition. All research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of medical information, trying to balance the research needs with the patients need for privacy of their medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process, but we may, however, disclose medical information

about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs, so long as the medical information they review does not leave Natividad. When necessary, we will ask for your specific permission if the researcher will have access to your name, address or other information that reveals who you are, or will be involved in your care at Natividad.

p. As Required By Law

We will disclose medical information about you when required to do so by federal, state or local law.

q. To Avert a Serious Threat to Health or Safety

We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

4. Special Situations

a. Organ and Tissue Donation

We may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

b. Military and Veterans

If you are a member of the U.S. Armed Forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

c. Workers' Compensation

We may release medical information about you for workers' compensation or similar programs. These programs provide benefits for work related injuries or illness.

d. Public Health Activities

We may disclose medical information about you for public health activities. These activities generally include the following:

- to prevent or control disease, injury or disability;
- to report births and deaths;
- to report the abuse or neglect of children, elders and dependent adults;
- to report reactions to medications or problems with products;

- to notify people of recalls of products they may be using;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law
- to notify emergency response employees regarding possible exposure to HIV/AIDS, to the extent necessary to comply with state and federal laws

e. Health Oversight Activities

We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

f. Lawsuits and Disputes

If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request (which may include written notice to you) or to obtain an order protecting the information requested.

g. Law Enforcement

We may release medical information if asked to do so by a law enforcement official:

- in response to a court order, subpoena, warrant, summons or similar process;
- to identify or locate a suspect, fugitive, material witness, or missing person;
- about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
- about a death we believe may be the result of criminal conduct;
- about criminal conduct at Natividad; and
- in emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime

h. Coroners, Medical Examiners and Funeral Directors

We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients of Natividad to funeral directors as necessary to carry out their duties.

i. National Security and Intelligence Activities

We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

j. Protective Services for the President and Others

We may disclose medical information about you to authorized federal officials so they may provide protection to the

President, other authorized persons or foreign heads of state or conduct special investigations.

k. Multidisciplinary Personnel Teams

We may disclose health information to a multidisciplinary personnel team relevant to the prevention, identification, management or treatment of an abused child and the child's parents, or elder abuse and neglect.

l. Special Categories of Information

In some circumstances, your health information may be subject to restrictions that may limit or preclude some uses or disclosures described in this notice. For example, there are special restrictions on the use or disclosure of certain categories of information - e.g., tests for HIV or treatment for mental health conditions or alcohol and drug abuse. Government health benefit programs, such as Medi-Cal, may also limit the disclosure of beneficiary information for purposes unrelated to the program.

m. Inmates

If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

5. Your Rights Regarding Medical Information About You

You have the following rights regarding medical information we maintain about you:

a. Right to Inspect and Copy

You have the right to inspect and/or obtain a copy of your medical information that may be used to make decisions about your care. Usually, this includes medical and billing records, but may not include some mental health information. You must submit your request in writing to Natividad Medical Center, Medical Records Department, 1441 Constitution Blvd., Salinas, CA 93906. If you have questions contact the Medical Records Department by dialing the main Natividad number.

You may be charged a fee for the costs of copying, mailing or other supplies associated with your request. We may deny your request to inspect and/or obtain a copy in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed. Another licensed health care professional chosen by Natividad will review your request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

b. Right to Amend

If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for Natividad.

To request an amendment your request must be made in writing, and submitted to the Natividad Medical Records Department, 1441 Constitution Blvd., Salinas, CA 93906.

In addition, you must provide a reason that supports your request. We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

- was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the medical information kept by or for Natividad;
- is not part of the information which you would be permitted to inspect and/or receive a copy; or

- Is accurate and complete

Even if we deny your request for amendment, you have the right to submit a written addendum, not to exceed 250 words, with respect to any item or statement in your record you believe is incomplete or incorrect. If you clearly indicate in writing that

you want the addendum to be made part of your medical record, we will attach it to your records and include it whenever we make a disclosure of the item or statement you believe to be incomplete or incorrect.

c. Right to an Accounting of Disclosures

You have the right to request an “accounting of disclosures.” This is a list of the disclosures we made of medical information about you other than our own uses for treatment, payment and health care operations, (as those functions are described above) and with other exceptions pursuant to the law. To request this list or accounting of disclosures, you must submit your request in writing to Natividad Medical Center, Medical Records Department, 1441 Constitution Blvd., Salinas, CA 93906. Your request must state a time period, which may not be longer than six years and may not include dates before April 14, 2003. The first list you request within a 12-month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

d. Right to Request Restrictions

You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had.

We are not required to agree to your request. If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment.

To request restrictions, you must make your request in writing at Natividad Medical Center, Medical Records Department, 1441 Constitution Blvd., Salinas, CA 93906. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse.

e. Right to Request Confidential Communications

You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. To request confidential communications, you must make your request in writing at Natividad Medical Center, Admitting Department, 1441 Constitution Blvd., Salinas, CA 93906.

We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

f. Right to a Paper Copy of This Notice

You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. You may obtain a copy of this notice at our website: www.natividad.com.

To obtain a paper copy of this notice: ask for it at any Admitting or Registration location.

6. Changes to this Notice

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current notice at Natividad. The notice will contain on the first page, in the top right-hand corner, the effective date.

7. Complaints

If you believe your privacy rights have been violated, you may file a complaint with Natividad or with the Secretary of the Department of Health and Human Services. To file a complaint with Natividad, contact the Compliance Officer by calling the main Natividad number. All complaints must be submitted in writing.

You will not be penalized for filing a complaint.

8. Other Uses of Medical Information

Other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose your medical information, you may revoke that permission, in writing, at any time. If you revoke your permission, this will stop any further use or disclosure of your medical information for the purposes covered by your written authorization, except if we have already acted in reliance on your permission. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

