

BUSINESS ASSOCIATE AGREEMENT AGREEMENT

This Business Associate Agreement Agreement (“**Agreement**”), effective as of the date of the last of the Parties to sign the signature page hereto (the “**Effective Date**”), is entered into by and between the following parties (each a “**Party**” and collectively the “**Parties**”):

<u>Covered Entity</u>		<u>Business Associate</u>
<i>Customer: San Bernardino County on behalf of Arrowhead Regional Medical Center</i>	<i>Philips:</i>	Philips Healthcare a division of Philips North America LLC and its Affiliates
<hr/> <i>Customer’s Principal Address: 400 N. Pepper Avenue, Colton, CA 92324</i>	<i>Philips’s Principal Address</i>	<hr/> 222 Jacobs Street, 3 rd Floor Cambridge, MA 02141

Section 1. BACKGROUND AND PURPOSE

- 1.1. The Parties have entered into a sales, service, rental or license agreement with respect to a Philips product, service, or software (the “Underlying Contract”), which provides for warranty or other service that may require Philips Healthcare a division of Philips North America LLA and its Affiliates (“Philips”) to be provided with, to have access to, and/or create Protected Health Information (“PHI”) that is subject to the federal regulations issued pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”), codified at 45 C.F.R. parts 160 and 164, and the Health Information Technology for Economic and Clinical Health (“HITECH”) (collectively, “HIPAA Rules”). This Agreement shall supplement and/or amend each of the Underlying Contract(s) only with respect to Philips’ receipt, use and creation of PHI under the Underlying Contract(s) to allow Customer and Philips to comply with the HIPAA Rules. Except as so supplemented and/or amended, the terms of the Underlying Contract(s) shall continue unchanged and shall apply with full force and effect to govern the matters addressed in this Agreement and in each of the Underlying Contract(s).

Section 2. DEFINITIONS

Unless otherwise specified herein, capitalized terms used in this Agreement shall have the same meanings as given in the HIPAA Rules, as and when amended from time to time.

- 2.1. “**Affiliate**” shall mean any corporation, company, or other entity, which: (i) is under the Control of a Party hereto; or (ii) has Control of a Party hereto; or (iii) is under common Control with a Party hereto, during the time such Control exists. For purposes of this Affiliate definition, “Control” means that more than fifty percent (50%) of the controlled

entity's shares or ownership interest representing the right to make decisions for such entity are owned or controlled, directly or indirectly, by the controlling entity.

- 2.2. **"Business Associate"** or **"BA"** shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean Philips.
- 2.3. **"Covered Entity"** or **"CE"** shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean the Customer.
- 2.4. **"HIPAA Rules"** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164 and HITECH. The **"HIPAA Privacy Rule"** is at 45 CFR, part 160 and part 164, subparts A and E. The **"HIPAA Security Rule"** is at 45 C.F.R. Parts 160 and 164. The **"HIPAA Breach Notification Rule"** is at 45 CFR Part 164 Subpart D.
- 2.5. **"PHI," "ePHI"** and **"uPHI"** shall mean Protected Health Information, Electronic Protected Health Information and Unsecured Protected Health Information, respectively, as defined in 45 C.F.R. §160.103, limited to the information Philips received from or created or received on behalf of Customer as Customer's Business Associate.
- 2.6. **"Philips"** means the listed Philips entity plus Affiliates of the listed Philips entity.
- 2.7. **"Subcontractor"** shall mean a "subcontractor" (as defined at 45 CFR 160.103) of Philips.
- 2.8. **Other.** All other capitalized terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules.

Section 3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

- 3.1. **General.** With regard to its use and/or disclosure of PHI, Business Associate agrees to:
 - (a) **Permissible Use/Disclosure.** Not Use or disclose PHI other than as permitted or required to perform the services in the Underlying Contract and by this Agreement or as Required By Law. Further, Business Associate shall not use PHI in any manner that would constitute a violation of the HIPAA Rules.;
 - (b) **Safeguards.** Use appropriate technical, administrative, and physical safeguards to prevent the unauthorized use or disclosure of PHI to comply with the Security Rule with respect to ePHI as of the Effective Date for Philips' obligations as a Business Associate, to prevent Use or Disclosure of PHI other than as provided for by this Agreement;
 - (c) **Policies.** In accordance with 45 C.F.R. section 164.316, maintain reasonable and appropriate written policies and procedures for its privacy and security program in order to comply with the HIPAA Rules;

- (d) **Training.** Provide appropriate training for its workforce on the requirements of the HIPAA Rules as those regulations affect the proper handling, use confidentiality and disclosure of the Covered Entity's PHI. Such training will include specific guidance relating to sanctions against workforce members who fail to comply with privacy and security policies and procedures and the obligations of the BA under the HIPAA Rules.
- (e) **Reports to Customer.** Report to Customer any Use or Disclosure of PHI not provided for by this Agreement of which it becomes aware, including Breaches of uPHI as required at 45 CFR 164.410, and any Security Incident affecting PHI of which it becomes aware;
- (f) **Subcontractors.** Enter into or have written agreements with agents and subcontractors to whom BA provides CE's PHI that impose the same restrictions and conditions that apply to Philips, in its capacity as the Business Associate, with respect to the PHI;
- (g) **Reporting of Improper Access, Use or Disclosure or Breach.** Every actual Breach shall be reported promptly and without unreasonable delay, but no later than ten (10) calendar days, to CE's Office of Compliance, consistent with the regulations under HITECH Act and California state law. Upon discovery of a Breach, BA shall complete the following actions:
 - i. Provide CE's Office of Compliance with the following information:
 - a) Date the Breach occurred;
 - b) Date the Breach was discovered;
 - c) To the extent required by state law, number of staff, employees, subcontractors, agents or other third parties and the names and titles of each person allegedly involved;
 - d) To the extent possible, the identification of each individual and contact information whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach
 - e) To the extent required by state law, number of potentially affected Individual(s) with contact information;
 - f) Description of how the Breach or suspected Breach allegedly occurred.
 - g) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 - h) Any information in Philips possession which Covered Entity is required to provide regarding steps individuals should take to protect themselves from potential harm resulting from the breach; and

- i) A brief description of what the Business Associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
 - ii. Make available to CE and governing State and Federal agencies in a time and manner designated by governing State and Federal agencies, any policies, procedures, internal practices and records relating to a Breach or suspected Breach;
- (h) **Mitigation.** BA shall have procedures in place to mitigate, to the extent practicable, any harmful effect that is known to BA of a use, access or disclosure of PHI by BA, its agents or subcontractors in violation of its policies and procedures or applicable state law and the HIPAA Rules
- (i) **Costs Associated to Breach.** BA shall be responsible for reasonable, actual **out of pocket** costs associated with **notification of** a Breach, including any required credit monitoring services provided to affected individuals.
- (j) **Designated Record Sets**
 - (i) Within ten (10) days of receiving a written request from Customer, make available to the Customer PHI necessary for Customer to respond to individuals' requests for access to PHI about them in the event that the PHI in Philips' possession constitutes a Designated Record Set.
 - (ii) Within the shorter of (1) the timeframe required by applicable law or (2) ten (10) calendar days of receiving a written request from Customer, make available to the Customer PHI for amendment and incorporate any amendments to the PHI in accordance with the Privacy Rule in the event that the PHI in Philips' possession constitutes a Designated Record Set.
- (k) **Accounting.** Within the shorter of (1) the timeframe required by applicable law or (2) ten (10) calendar days of receiving a written request from Customer in response to a request from an Individual, make available to the Customer the information required for the Customer to provide an accounting of Disclosures as necessary to satisfy its obligations as a Covered Entity under 45 CFR 164.528;
- (l) **Inspection by Secretary.** Make its internal practices, including policies and procedures, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.
- (m) **Indemnification.** Business Associate shall defend, indemnify and hold the Covered Entity harmless from and against any and all (a) out of pocket costs and expenses, including reasonable attorneys' fees, to fulfill any notification obligations imposed on Covered Entity to the extent arising from Business Associate's unauthorized use or disclosure of PHI, (b) any third party lawsuit, claim, action, losses, liability, costs to the extent due to Business Associate's failure to comply with HIPAA and the terms of this Agreement, and (c) penalties

imposed by a federal or state governing agency against Covered Entity to the extent such penalty is imposed upon Covered Entity citing Business Associate's acts or omissions of its obligations hereunder as the basis for imposing such penalty against Covered Entity.

- (n) **Insurance.** Business Associate agrees that it shall continually maintain appropriate insurance coverage to cover any liabilities that may arising under this Agreement and will provide its COI upon request.
- (o) **Judicial or Administrative Proceedings.** CE may terminate the Underlying Contract, effective immediately, if BA is convicted for a violation of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws
- (p) **Assistance in Litigation or Administrative Proceedings.** BA shall make itself reasonably available to CE to assist in the event of litigation or administrative proceedings being commenced against CE, its directors, officers, or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where BA or its subcontractor, employee or agent is a named adverse party.

Section 4. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

Except as otherwise specified in this Agreement, Philips may:

- 4.1. General.** Use or disclose PHI as Philips deems necessary to perform its obligations under the Underlying Contracts or as otherwise permitted or required by law. Such use, disclosure or request of PHI shall utilize a limited data set if practicable or otherwise the minimum necessary PHI to accomplish the intended results of the use, disclosure or request. Philips also agrees to follow appropriate minimum necessary policies in the performance of its obligations under this agreement.
- 4.2. Required by Law.** Use or disclose PHI as Required By Law.
- 4.3. Proper Management and Administration**
 - (a) Use the PHI in its possession for its proper management and administration and to carry out the legal responsibilities of Philips;
 - (b) Disclose the PHI in its possession to a third party for the purpose of Philips' proper management and administration or to carry out the legal responsibilities of Philips, provided that the disclosures are required by law or Philips obtains, in writing, prior to making any disclosure to the third party, reasonable assurances from the third party regarding the confidential handling of such PHI as required under the HIPAA Rules, including entering into an agreement with the third-party to notify BA immediately of any Breaches of the PHI;
- 4.4. Data Aggregation.** Provide Data Aggregation services relating to the health care

operations of the Customer as permitted by law; and

- 4.5. **De-Identification.** De-identify any PHI obtained by Philips under this Agreement, and use and disclose such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule.
- 4.6. **Marketing.** Philips may not use or disclose PHI received by CE under the Underlying Contract for marketing or fundraising purposes;
- 4.7. **Sale.** BA shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CE and as permitted by the HITECH Act (42 U.S.C. section 17935(d)(2); and 45 C.F.R. section 164.508); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to this Agreement.

Section 5. TERMINATION

- 5.1. **Termination.** This Agreement shall terminate on (a) the date that the last of the Underlying Contracts terminates or expires or (b) on the date Covered Entity terminates this Agreement pursuant to the provisions in this Agreement, whichever is sooner.
- 5.2. **Termination by Customer.** Should Customer become aware of a breach of a material term of this Agreement by Philips, Customer shall provide Philips with written notice of such breach in sufficient detail to enable Philips to understand the specific nature of the breach, and provide Philips with at least 30 days to cure such breach. Customer shall be entitled to terminate the Underlying Contract associated with such breach if, after Customer provides the notice to Philips, Philips fails to cure the breach within a reasonable time period specified by Customer in such notice; provided, however, that such time period specified by Customer shall be based on the nature of the breach involved, and shall not be less than 30 days. If Customer determines that Business Associate has breached the terms of this Agreement and such breach has not been cured, but Customer determines that termination of the Underlying Contract(s) is not feasible, Customer may report such breach to the U.S. Department of Health and Human Services. CE may immediately terminate this Agreement and, if required by applicable law, any Underlying Contract, if BA has breached a material term of this Agreement or violates the HIPAA Rules and cure is not reasonably possible.
- 5.3. **Effect of Termination.** Upon termination of this Agreement for any reason, Philips, with respect to PHI received from Customer, or created, maintained, or received by Philips on behalf of Customer, shall:
 - (a) Retain only that PHI which is necessary for Philips to continue its proper management and administration or to carry out its legal responsibilities;
 - (b) Return to Customer or destroy the remaining PHI that Philips still maintains, if it is feasible to do so;
 - (c) In the event the BA determines that returning the PHI is not feasible, the BA

shall provide the CE with written notification of the conditions that make return not feasible. Additionally, the BA must follow established policies and procedures to ensure PHI is safeguarded and disposed of adequately in accordance with 45 C.F.R. section 164.310, and must submit to the CE a certification of destruction of PHI.

- (d) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to ePHI that cannot be returned or destroyed to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Philips retains the PHI;
- (e) Not use or disclose the PHI retained by Philips other than for the purposes for which such PHI was retained and subject to the same conditions set out in this Agreement which applied prior to termination; and
- (f) Return to Customer or destroy the PHI retained by Philips when it is no longer needed by Philips for its proper management and administration or to carry out its legal responsibilities.

5.4. *Survival.* The provisions of this Agreement which by their nature are intended to survive termination or expiration, shall remain in full force and effect following the termination or expiration of this Agreement and Underlying Contract. Such provisions shall survive and continue to bind the parties in accordance with their terms, notwithstanding any termination or expiration of this Agreement or the Underlying Contract.

Section 6. MISCELLANEOUS

6.1. *Amendment.* The parties acknowledge that state and federal laws related to privacy and security of PHI are rapidly evolving and that amendment of this Agreement may be required to ensure compliance with such developments. The parties shall negotiate in good faith to amend this Agreement when and as necessary to comply with applicable laws. To the extent an amendment to this Agreement is required by law and this Agreement has not been so amended to comply with the applicable law in a timely manner, the amendment required by law shall be deemed to be incorporated into this Agreement automatically and without further action required by either of the parties. Subject to the foregoing, this Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed and agreed to by BA and CE..

6.2. *No Third Party Beneficiaries.* Nothing in this Agreement shall confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

6.3. *Interpretation.* The terms of this Agreement shall prevail in the case of any conflict with the terms of any Underlying Contract to the extent necessary to allow the parties to comply with the HIPAA Rules. The bracketed citations to the HIPAA Rules in several paragraphs of this Agreement are for reference only and shall not be relevant in interpreting any provision of this Agreement. Any ambiguity in this Agreement shall be

resolved to permit the parties to comply with the Privacy and Security Rules, the HITECH Act, and all applicable patient confidentiality regulations.

- 6.4. *Compliance with State Law.*** In addition to HIPAA and all the HIPAA Rules, BA acknowledges that BA and CE may have confidentiality and privacy obligations under State law, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq. (“CMIA”). If any provisions of this Agreement or the HIPAA Rules conflict with CMIA or any other California State law regarding the degree of protection provided for PHI and patient medical records, then BA shall comply with the more restrictive requirements.
- 6.5. *Remedies.*** BA agrees that CE shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which CE may have at law or in equity in the event of an unauthorized use, access or disclosure of PHI by BA or any agent or subcontractor of BA that received PHI from BA.
- 6.6. *Data Ownership.*** The PHI shall be and remain the property of the CE. BA agrees that it acquires no title or rights to the PHI.
- 6.7. *Counterparts.*** This Agreement may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Agreement. The parties shall be entitled to sign and transmit an electronic signature of this Agreement (whether by facsimile, PDF or other email transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Agreement upon request.

Section 7. RESPONSIBILITIES OF THE COVERED ENTITY

- 7.1** CE shall notify BA of any of the following, to the extent that such may affect BA’s use, access, maintenance or disclosure of PHI:
- (a) Any limitation(s) in CE’s notice of privacy practices in accordance with 45 C.F.R. section 164.520.
 - (b) Any changes in, or revocation of, permission by an individual to use, access or disclose PHI.
 - (c) Any restriction to the use, access or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. section 164.522.

[SIGNATURE PAGE FOLLOWS]

COVERED ENTITY

PHILIPS

Signature

Name (*print*): Dawn Rowe

Title: Chair, Board of Supervisors

Date: _____

ADDRESS FOR NOTICE:

Arrowhead Regional Medical Center
400 N. Pepper Avenue
Colton, CA 92324
Attn: ARMC Chief Executive Officer

Signature

Name (*print*): Eric Douma

Title: Contracts Manager

Date: _____

ADDRESS FOR NOTICE:

Philips Healthcare
222 Jacobs Street, 3rd Floor
Cambridge, MA 02141
Attn: HIPAA Coordinator
Fax: 800-947-3299