

## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement) is entered into by and between the County of San Bernardino on behalf of Arrowhead Regional Medical Center (hereinafter, Covered Entity) and Surescripts, LLC, a Delaware limited liability company (hereinafter, Business Associate) as of the date of last signature below (Effective Date).

### RECITALS

**WHEREAS**, Covered Entity (CE) and Business Associate (BA) have entered, or will enter into, one or more contractual relationships (collectively, Contract for Services) which may require CE to disclose certain information to BA, which may include Protected Health Information (PHI); and

**WHEREAS**, CE and BA intend to protect the privacy and provide for the security of the PHI disclosed to BA pursuant to this Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (HITECH Act), their implementing regulations, and other applicable laws; and

**WHEREAS**, The Privacy Rule and the Security Rule require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, sections 164.314, subdivision (a), 164.502, subdivision (e), and 164.504, subdivision (e) of the Code of Federal Regulations (C.F.R.) and as contained in this Agreement; and

**WHEREAS**, Pursuant to HIPAA and the HITECH Act, BA shall fulfill the responsibilities of this Agreement by being in compliance with the applicable provisions of the HIPAA Standards for Privacy and Security of PHI set forth at 45 C.F.R. sections 164.530 (Administrative Requirements), 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards), 164.316 (Policies and Procedures and Documentation Requirements), and, 164.400, et seq. and 42 United States Code (U.S.C.) section 17932 (Breach Notification Rule), in the same manner as they apply to a CE under HIPAA.

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

#### A. Definitions

Unless otherwise specified herein, capitalized terms used in this Agreement shall have the same meanings as given in the Privacy Rule, the Security Rule, the Breach Notification Rule, and HITECH Act, as and when amended from time to time.

1. Breach shall have the same meaning given to such term under the HIPAA Regulations [45 C.F.R. §164.402] and the HITECH Act [42 U.S.C. §§17921 et seq.], and as further described in California Civil Code section 1798.82.

2. Business Associate (BA) shall have the same meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to 42 U.S.C. section 17921 and 45 C.F.R. section 160.103.
3. Covered Entity (CE) shall have the same meaning given to such term as under the Privacy Rule and Security Rule, including, but not limited to 45 C.F.R. section 160.103.
4. Designated Record Set shall have the same meaning given to such term under 45 C.F.R. section 164.501.
5. Electronic Protected Health Information (ePHI) means PHI that is maintained in or transmitted by electronic media as defined in the Security Rule, 45 C.F.R. section 164.103.
6. Individual shall have the same meaning given to such term under 45 C.F.R. section 160.103.
7. Privacy Rule means the regulations promulgated under HIPAA by the United States Department of Health and Human Services (HHS) to protect the privacy of Protected Health Information, including, but not limited to, 45 C.F.R. Parts 160 and 164, subparts A and E.
8. Protected Health Information (PHI) shall have the same meaning given to such term under 45 C.F.R. section 160.103, limited to the information received from, or created or received by Business Associate from or on behalf of, CE.
9. Security Rule means the regulations promulgated under HIPAA by HHS to protect the security of ePHI, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, subparts A and C.
10. Unsecured PHI shall have the same meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act, including, but not limited to 42 U.S.C. section 17932, subdivision (h).

**B. Obligations and Activities of BA**

**1. Permitted Uses and Disclosures**

- i. CE shall disclose PHI to BA for the purposes set forth in detail in the Contract for Services.
- ii. BA may use and disclose PHI: (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) for purposes of Treatment, Payment and Operations (TPO); (iv) as required by law; or (v) for Data Aggregation purposes for the Health Care Operations of CE. Prior to making any other disclosures, BA must obtain a written authorization from the Individual.
- iii. If BA discloses PHI to a third party, BA must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such PHI will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify BA of any breaches of confidentiality of the PHI, to the extent it has obtained knowledge of such breach. [42 U.S.C. section 17932; 45 C.F.R.

sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)]

## 2. Prohibited Uses and Disclosures

- i. BA shall not use, access or further disclose PHI other than as permitted or required by this Agreement or as required by law. Further, BA shall not use PHI in any manner that would constitute a violation of the Privacy Rule or the HITECH Act. BA shall disclose to its employees, subcontractors, or other third parties, and request from CE, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder.
- ii. BA shall not use or disclose PHI for fundraising or marketing purposes.
- iii. BA shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates. (42 U.S.C. section 17935(a) and 45 C.F.R. section 164.522(a)(1)(i)(A).)
- iv. 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.

## 3. Appropriate Safeguards

- i. BA shall implement appropriate safeguards to prevent the unauthorized use or disclosure of PHI, including, but not limited to, administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of the PHI BA creates, receives, maintains, or transmits on behalf of the CE, in accordance with 45 C.F.R. sections 164.308, 164.310, 164.312 and 164.316. [45 C.F.R. sections 164.504(e)(2)(ii)(b) and 164.308(b).]
- ii. In accordance with 45 C.F.R. section 164.316, BA shall maintain reasonable and appropriate written policies and procedures for its privacy and security program in order to comply with the standards, implementation specifications, or any other requirements of the Privacy Rule and applicable provisions of the Security Rule.
- iii. BA shall provide appropriate training for its workforce on the requirements of the Privacy Rule and Security Rule as those regulations affect the proper handling, use confidentiality and disclosure of 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 with respect to the handling, use and disclosure of PHI.

## 4. Subcontractors

BA shall enter into written agreements with subcontractors to whom BA provides CE's PHI that impose substantially the same restrictions and conditions on such subcontractors that apply to BA with respect to such PHI, and that require compliance with all appropriate safeguards as found in this Agreement.

5. Reporting of Improper Access, Use, or Disclosure of PHI or Breach of Unsecured PHI, or Security Incident.

BA agrees to provide notice to CE without unreasonable delay, but no later than ten (10) business days after determining that a Breach has occurred. The notification shall include, to the extent possible, sufficient information for CE to understand the nature of the Breach such as descriptions of: (i) the Breach, including the date of the Breach and the date of discovery of the Breach, if known; (ii) a general description of the type of message content involved, if applicable; (iii) the individuals or records which are or reasonably could be impacted by the Breach; (iv) any steps the individuals whose PHI was breached should take to protect themselves from potential harm resulting from the Breach; (v) actions taken by BA to investigate and mitigate the Breach; (vi) current status of the Breach and corrective action being undertaken and plans to prevent similar breaches; and (vii) contact procedures for individuals whose PHI was breached to ask questions or learn additional information about the Breach, if applicable. BA shall supplement the information contained in the notification as it becomes available and shall cooperate with CA as necessary. This Section is in addition to BA's obligations and limitations under relevant security incident, breach notification, or confidentiality provisions of Applicable Law. For purposes of this Section, the term "Breach" has the same meaning as defined in 45 C.F.R. § 164.402 and, therefore, is limited to a breach of "Unsecured PHI." Unsecured PHI is protected health information that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through use of technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.

6. Access to PHI

To the extent BA maintains a Designated Record Set on behalf of CE, BA shall make PHI maintained by BA in Designated Record Sets available to CE for inspection and copying within ten (10) days of a request by CE to enable CE to fulfill its obligations under the Privacy Rule. If BA maintains ePHI, BA shall provide such information in electronic format to enable CE to fulfill its obligations under the HITECH Act. If BA receives a request from an Individual for access to PHI, BA shall forward such request to CE within five (5) business days of receipt. Following receipt of such notice from BA, CE shall handle such request from the Individual.

7. Amendment of PHI

If BA maintains a Designated Record Set on behalf of the CE, BA shall make any amendment(s) to PHI in a Designated Record Set that the CE directs or agrees to, pursuant to 45 C.F.R. section 164.526. If BA receives a request from an Individual to amend PHI, BA shall forward such request to CE within five (5) business days of receipt. Following receipt of such notice from BA, CE shall handle such request from the Individual.

8. Access to Records

BA shall make internal practices, books, and records, including policies and procedures, relating to the use, access and disclosure of PHI received from, or created or received by BA on behalf of, CE available to the Secretary of HHS, in a time and manner designated by the Secretary, for purposes of the Secretary determining CE's and or

BA's compliance with the Privacy Rule and Security Rule and patient confidentiality regulations. Any documentation provided to the Secretary shall, unless otherwise prohibited by law, also be provided to the CE upon written request.

9. Accounting for Disclosures

BA and its subcontractors shall document disclosures of PHI and information related to such disclosures as required by HIPAA. This requirement does not apply to disclosures made for purposes of TPO. BA shall provide an accounting of disclosures to CE in the time and manner designated by the CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its subcontractors for at least six (6) years prior to the request. At a minimum, the information collected and maintained 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 purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

10. Termination

CE may terminate this Agreement, and any related agreements, if CE determines that BA has breached a material term of this Agreement, and BA has failed to cure the breach or end the violation within thirty (30) calendar days following receipt of breach notice from CE .

11. Return of PHI

Upon termination of this Agreement for any reason, the parties hereby acknowledge that returning or destruction of the PHI received by BA from CE is not feasible, in part due to CMS regulations that require certain information be maintained by Business Associates for audit purposes for a period of ten (10) years, and that, therefore, BA may retain a copy of such PHI. 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. For destruction of ePHI, the National Institute of Standards and Technology (NIST) guidelines must be followed. BA further agrees to extend any and all protections, limitations, and restrictions contained in this Agreement, to any PHI retained by BA or its subcontractors, or employees after the termination of this Agreement, and to limit any further use, access or disclosures.

12. Breach by the CE

Pursuant to 42 U.S.C. section 17934, subdivision (b), if the BA is aware of any activity or practice by the CE that constitutes a material Breach or violation of the CE's obligations under this Agreement, and such violation continues for thirty (30) calendar days after written notice of such breach has been provided to CE by BA and the CE continues with non-compliant activity, the BA must terminate the Agreement (if feasible) and report the violation to the Secretary of HHS.

13. 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, or subcontractors in violation of the requirements of this Agreement.

#### 14. Costs Associated to Breach

BA shall reimburse CE for the actual costs associated with providing legally required notification of a Breach of PHI directly attributable to or cause by BA or its subcontractors. Costs shall be based upon the required notification type as deemed appropriate and necessary by the CE. CE shall determine the method to invoice the BA for said costs. Costs shall incur at the current rates and may include, but are not limited to the following:

- Postage;
- Alternative means of notice;
- Media notification; and
- Credit monitoring services for not more than twelve (12) months following date breach notification is provided by CE.

#### 15. Direct Liability

BA may be held directly liable under HIPAA for impermissible uses and disclosures of PHI; failure to provide breach notification to CE; failure to provide access to a copy of PHI or ePHI to CE or Individual; failure to disclose PHI to the Secretary of HHS when investigating BA's compliance with HIPAA; failure to provide an accounting of disclosures; and, failure to enter into a business associate agreement with subcontractors.

#### 16. Indemnification

BA agrees to indemnify, defend and hold harmless CE and its authorized officers, directors, employees, agents and subcontractors from any and all third-party claims, actions, losses, damages, penalties, injuries, costs and expenses (including costs for reasonable attorney fees) that are caused by or result from the acts or omissions of BA, its officers, employees, and subcontractors, with respect to the use, access, maintenance or disclosure of CE's PHI, including without limitation, any Breach of PHI and the actual expenses incurred by CE in providing legally required Breach notifications.

#### 17. Judicial or Administrative Proceedings

Either party may terminate this Agreement, effective immediately, if (i) the other party is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws or (ii) a finding or stipulation is made in any administrative or civil proceeding in which the other party has been joined that such party has violated any standard or requirement of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws.

#### 18. Insurance

In addition to any general and/or professional liability insurance coverage required of BA under the Contract for Services, BA shall provide appropriate liability insurance coverage during the term of this Agreement to cover any and all claims, causes of action, and demands whatsoever made for loss, damage, or injury to any person arising from the breach of the security, privacy, or confidentiality obligations of BA, its subcontractors or employees, under this Agreement and under HIPAA 45 C.F.R. Parts 160 and 164, Subparts A and E.

## 19. Assistance in Litigation or Administrative Proceedings

BA shall make itself, and any subcontractors, or employees, assisting BA in the performance of its obligations under the Agreement, available to CE, to testify as witnesses, or otherwise, 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, or employee is a named adverse party.

### **C. Obligations of CE**

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:
  - i. Any limitation(s) in CE's notice of privacy practices in accordance with 45 C.F.R. section 164.520.
  - ii. Any changes in, or revocation of, permission by an Individual to use, access or disclose PHI.
  - iii. 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. In the event BA is unable to accommodate such restriction, BA shall promptly notify CE in writing and BA may terminate this Agreement upon thirty (30) calendar days' notice without penalty.

### **D. General Provisions**

#### 1. 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 subcontractor of BA that received PHI from BA.

#### 2. Ownership

The PHI shall be and remain the property of the CE. BA agrees that it acquires no title or rights to the PHI.

#### 3. Regulatory References

A reference in this Agreement to a section in the Privacy Rule and Security Rule and patient confidentiality regulations means the section as in effect or as amended.

#### 4. No Third-Party Beneficiaries

Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CE, BA and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

#### 5. Amendment

The parties acknowledge that state and federal laws related to privacy and security of PHI are rapidly evolving and that amendment of the Contract for Services or 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. If either party does not agree to so amend this Agreement within

30 days after receiving a request for amendment from the other, either party may terminate the Agreement upon written notice. 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. Interpretation

Any ambiguity in this Agreement shall be resolved to permit both parties to comply with the Privacy and Security Rules, the HITECH Act, and all applicable patient confidentiality regulations.

7. Compliance with State Law

In addition to HIPAA and all applicable HIPAA Regulations, 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 HIPAA Regulations or the HITECH Act conflict with CMIA or any other California State law regarding the degree of protection provided for PHI and patient medical records, then both parties shall comply with the more restrictive requirements.

8. Survival

The respective rights and obligations and rights of CE and BA relating to protecting the confidentiality of an Individual's PHI shall survive the termination of the Contract for Services or this Agreement.

9. Governing Law

This Agreement shall be governed by and construed in all aspects in accordance with the laws of the State of California without regard to principles of conflicts of laws.

10. Signatures

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.

The undersigned affirms that he/she is a duly authorized representative of the party for which he/she is signing and has authority to execute this Agreement on behalf of such party.

COUNTY OF SAN BERNARDINO

► */s/*  
\_\_\_\_\_  
Curt Hagman, Chairman, Board of Supervisors

*/d/*  
Dated: \_\_\_\_\_  
SIGNED AND CERTIFIED THAT A COPY OF THIS  
DOCUMENT HAS BEEN DELIVERED TO THE  
CHAIRMAN OF THE BOARD

Lynna Monell  
Clerk of the Board of Supervisors  
of the County of San Bernardino

By */s/* \_\_\_\_\_  
Deputy

SURESCRIPTS, LLC

\_\_\_\_\_  
*(Print or type name of corporation, company, contractor, etc.)*

By ►   
\_\_\_\_\_  
*(Authorized signature - sign in blue ink)*

Thomas M. Farah

Name \_\_\_\_\_  
*(Print or type name of person signing contract)*

Title General Counsel  
\_\_\_\_\_  
*(Print or Type)*

Dated: */* March 10, 2021  
\_\_\_\_\_  
2550 South Clark Street, 10<sup>th</sup> Floor

Address \_\_\_\_\_  
Arlington, VA 22202