

## **BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (the "Agreement") is made effective on this 21st day of January, 2014, by and between St. Charles Health System, Inc. ("Covered Entity"), and Milliman, Inc. ("Business Associate"). In this Agreement, Covered Entity and Business Associate may each be referred to as a "Party" and may collectively be referred to as the "Parties".

### **WITNESSETH:**

**WHEREAS**, the HIPAA Rules (as defined below), as well as applicable state information privacy and security laws and regulations, impose upon covered entities and their business associates certain obligations regarding the safeguarding, use, and disclosure of protected health information ("PHI"), as that term is defined by the HIPAA Rules; and

**WHEREAS**, the Parties wish to enter into or have entered into one or more service agreements (individually or collectively, the "Service Agreement"), pursuant to which Business Associate may access, use and/or disclose PHI from or on behalf of Covered Entity; and

**WHEREAS**, the Parties are committed to complying with the HIPAA Rules and applicable federal state information privacy and security laws and regulations (collectively, the "Privacy and Security Rules") and, to that end, desire to enter into this Agreement;

**NOW, THEREFORE**, in consideration of the Parties' continuing obligations under the Service Agreement and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

### **I. DEFINITIONS**

Except as otherwise defined herein, any and all capitalized terms in this Agreement shall have the definitions set forth in the HIPAA Rules and ORS 192.556. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the Privacy and Security Rules, as amended, the mandatory provisions of the Privacy and Security Rules shall control. Where the provisions of this Agreement are different from those mandated in the Privacy and Security Rules, but are nonetheless permitted by the Privacy and Security Rules, the provisions of this Agreement shall control.

The term "Covered Entity" 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 St. Charles Health System, Inc., St. Charles Health Plan, Inc., St. Charles Management Services Organization, LLC, and all of their respective divisions, affiliates, and workforce members.

The HIPAA Rules shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and 164.

Business Associate acknowledges and agrees that this Agreement pertains to, and that, for purposes of this Agreement, PHI shall mean, all PHI, in paper, electronic and any other form, created or received by Business Associate from or on behalf of Covered Entity or any of Covered Entity's business units.

### **II. PRIVACY REQUIREMENTS**

(a) Business Associate agrees:

(i) to use or disclose any PHI in a manner consistent with Covered Entity's minimum necessary policies and procedures and solely: (1) for meeting its obligations as set forth in any agreements between the Parties evidencing their business relationship, or (2) as required by applicable law, rule or regulation, or as otherwise permitted under this Agreement, the Service Agreement (if consistent with this Agreement and the Privacy and Security Rules), or the Privacy and Security Rules, and (3) as would be permitted by the Privacy and Security Rules if such use or disclosure were made by Covered Entity;

(ii) to return or destroy at its own costs, at termination of this Agreement, the Service Agreement (or any similar documentation of the business relationship of the Parties), or upon request of Covered Entity, whichever occurs first, all PHI received from or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form and not retain copies of such information, or if such return or destruction is not feasible with respect to any portion of PHI (the "Retained PHI"), Business Associate shall: (1) continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 and other applicable provisions of the Privacy and Security Rules with respect to the Retained PHI for as long as Business Associate retains the same; (2) not use or disclose the Retained PHI other than for the purposes for which such PHI was retained and subject to the same conditions set out at Section II(b)(i)-(ii) that applied prior to termination; and (3) return the Retained PHI to Covered Entity when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities;

(iii) in accordance with 45 CFR §§164.502(e)(1)(ii) and 164.308(b)(2), to ensure that its agents, including a subcontractor or business associate, to whom it provides PHI received from or created by Business Associate on behalf of Covered Entity, agree to substantially the same restrictions and conditions that apply to Business Associate with respect to such information;

(iv) to ensure that its employees' actions or omissions do not cause Business Associate to breach the terms of this Agreement;

(v) to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement;

(vi) to report to Covered Entity promptly, but in no case later than ten (10) business days after discovery, any use or disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware, including breaches of unsecured PHI as required at 45 CFR §164.410. Covered Entity will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media; and

(vii) to comply with the requirements of Subpart E of 45 CFR Part 164 when carrying out any duties for or on behalf of Covered Entity.

(b) Notwithstanding the prohibitions set forth above, Business Associate may use and disclose PHI as follows:

(i) if necessary, for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that as to any such disclosure, the following requirements are met: (1) the disclosure is required by law; or (2) Business Associate has entered with the person to whom PHI is disclosed into an agreement that contains the same restrictions and conditions that apply to Business Associate with respect to such information;

(ii) for data aggregation services, if the same are to be provided by Business Associate for the health care operations of Covered Entity pursuant to an agreement between the Parties evidencing their business relationship. For purposes of this Agreement, data aggregation services means the combining by Business Associate of PHI of Covered Entity with PHI of another covered entity in connection with the performance of data analyses that relate to the health care operations of the respective covered entities;

(iii) to create a Limited Data Set for the purpose of performing its obligations and services for Covered Entity, provided that Business Associate otherwise complies with the provisions of this Agreement; and

(iv) to Deidentify PHI in accordance with the requirements of the Privacy Rule and maintain such deidentified health information indefinitely; provided the de-identified health information is not subsequently disclosed, including sold, to third parties and that all identifiers are destroyed or returned in accordance with this Agreement.

(c) Covered Entity agrees:

(i) to not provide Business Associate with more PHI than that which is minimally necessary for Business Associate to provide the services and, where possible, Covered Entity shall provide any PHI needed by Business Associate to perform the services in the form of a Limited Data Set, in accordance with the HIPAA regulations; and

(ii) to not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or the Security Rule if done by Covered Entity, except as otherwise expressly permitted in section II(b) above.

### III. SECURITY REQUIREMENTS

(a) Business Associate agrees:

(i) to implement administrative safeguards, physical safeguards and technical safeguards, including, without limitation, appropriate data encryption methods and technologies (collectively, "Safeguards") that comply with Subpart C of 45 CFR Part 164 and that reasonably and appropriately protect the confidentiality, integrity and availability of any electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity ("ePHI");

(ii) to enter with any person to whom the ePHI is disclosed into an agreement that contains substantially the same restrictions and conditions that apply to Business Associate with respect to such ePHI, including, without limitation, the obligation to implement appropriate Safeguards; and

(iii) to report to Covered Entity any successful Security Incident which comes to the attention of Business Associate and involves ePHI. The parties acknowledge and agree that this section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but unsuccessful Security Incidents of which no additional notice to Covered Entity shall be required. Unsuccessful Security Incidents shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as such incidents do not result in unauthorized access, use or disclosure of Covered Entity's PHI.

(b) In addition to the foregoing, Business Associate agrees that, while present at any Covered Entity facility and/or when accessing Covered Entity's computer network(s), it and all of its employees, agents, representatives and subcontractors shall at all times comply with any network access and other information privacy and security practices, procedures and/or policies of which it has advance notice established by Covered Entity pursuant to the Privacy and Security Rules.

### IV. AUDITING AND REPORTING REQUIREMENTS

Business Associate agrees that the Secretary of Health and Human Services and, with prior notice, Covered Entity shall have the right to audit and otherwise assess the internal practices, policies, books and records of Business Associate to ensure that Covered Entity is complying with the terms of the Privacy and

Security Rules. Unless Business Associate is instructed by a law enforcement official to do otherwise, Business Associate shall notify Covered Entity promptly, but in no case later than ten (10) days, following discovery of any Breach of unsecured PHI. Such notification shall include the identification of each individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Such notification shall also include, as soon as and to the extent that such information is available to Business Associate: (a) a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, (b) a description of the types of PHI involved in the Breach, (c) any steps that individuals should take to protect themselves from potential harm resulting from the Breach, (d) a brief description of what Business Associate is doing to investigate the Breach, mitigate harm to individuals, and protect against further Breaches, and (e) any other information Covered Entity is required to include in its Notice to Individuals, if applicable.

## **V. AVAILABILITY OF PHI**

To the extent that it maintains PHI in a Designated Record Set, Business Associate agrees upon request from Covered Entity to make available PHI to Covered Entity to the extent and in the manner required by 45 C.F.R. §164.524. Business Associate agrees upon request from Covered Entity to make PHI available to Covered Entity for amendment and to incorporate amendments to PHI in accordance with the requirements set forth in 45 C.F.R. §164.526. In addition, Business Associate agrees to make PHI available for the purpose of creating an accounting of disclosures, as required by 45 C.F.R. §164.528. Business Associate will promptly notify Covered Entity when a request for access or amendment to PHI or accounting of disclosures is received and shall reasonably cooperate with Covered Entity to facilitate Covered Entity's response to such request.

## **VI. TERMINATION**

Covered Entity may immediately terminate this Agreement and the Service Agreement if Covered Entity determines that Business Associate has breached a material term of this Agreement. Alternatively, Covered Entity may: (i) provide Business Associate with written notice of the alleged material breach; and (ii) afford Business Associate thirty (30) days to cure such breach to the satisfaction of Covered Entity. If Business Associate fails to cure the breach within the 30-day cure period, then Covered Entity may terminate this Agreement and the Service Agreement immediately. Covered Entity shall have the right to report any breach to the Secretary of Health and Human Services as provided for under 45 C.F.R. §164.504. This Agreement will automatically terminate without any further action of the Parties upon the termination or expiration of the last Service Agreement in effect between the Parties.

## **VII. MISCELLANEOUS**

This Agreement shall replace all prior business associate agreements between the Parties, whether such agreements are stand-alone agreements or are incorporated into other agreements, and shall constitute the entire agreement of the parties hereto with respect to the subject matter hereof. Except as expressly stated herein or the Privacy and Security Rules, the Parties do not intend to create any rights in any third parties. The obligations of Business Associate under this Agreement shall survive the expiration, termination, or cancellation of this Agreement, the Service Agreement and/or the business relationship of the Parties, and shall continue to bind Business Associate, its agents, employees, contractors, successors, and assigns as set forth herein.

This Agreement may be amended or modified only in writing signed by the Parties. No Party may assign its rights and obligations under this Agreement without the prior written consent of the other Party. None of the provisions of this Agreement are intended to create, nor will they be deemed to create, any relationship between the Parties other than that of independent parties contracting with each other solely for the purpose of effectuating the provisions of this Agreement and any other agreements between the Parties evidencing their relationship. This Agreement will be governed by the laws of Oregon to the extent not superseded by applicable federal law. No change, waiver or discharge of any liability or obligation hereunder, on any one or more occasions, shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.


In the event that any terms of this Agreement are inconsistent with the terms of any underlying agreement between the parties, then the terms of this Agreement shall control.

In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event that either Party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the Privacy and Security Rules, then such Party shall notify the other Party of its belief in writing. For a period of up to thirty (30) days, the Parties shall address in good faith such concern and amend the terms of this Agreement, if necessary, to bring it into compliance. If, after such thirty-day period, the Agreement fails to comply with the Privacy and Security Rules, then either Party has the right to terminate this Agreement upon written notice to the other Party. A reference in this Agreement to a section in the Privacy and Security Rules means the section as in effect or as amended, and for which compliance is required.


Each party agrees to defend, cover, and indemnify the other party against, all out-of-pocket costs and expenses, including, without limitation, reasonable attorneys' fees and breach notification costs, which result directly or indirectly from the indemnifying party's breach of the terms and conditions of this Agreement. Covered Entity will have sole discretion to determine whether any use or disclosure not provided for by this Agreement is a breach of unsecured PHI under Subpart D of 45 CFR Part 164.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year written above.

**COVERED ENTITY:**  
St. Charles Health System, Inc.

By:   
Karen M. Shepard  
Title: Executive V.P., Finance / CFO

**BUSINESS ASSOCIATE:**  
Milliman, Inc.

By:   
Title: Principal and Consulting Actuary