

## **BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement ("Agreement") is entered into as of January 31, 2017 ("Effective Date") by and between WellSpan Population Health Services, ("Business Associate") and Milliman Inc., on behalf of itself and its affiliates ("Subcontractor"). Each of the Business Associate and Subcontractor may be referenced in this Agreement as a "Party" and collectively as the "Parties."

To the extent Protected Health Information received from Business Associate or created or received by Subcontractor on behalf of Business Associate may be needed for Subcontractor to perform the Underlying Services requested by Business Associate and described in the Underlying Services Agreement, the Parties, intending to be legally bound, hereby agree as follows:

### **1. Definitions**

1.1 Except as otherwise defined in this Agreement, all capitalized terms used in this Agreement shall have the meanings set forth in HIPAA.

1.2 "Breach" shall mean the acquisition, access, use or disclosure of Protected Health Information ("PHI") in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of the PHI as defined, and subject to the exceptions set forth, in 45 CFR § 164.402.

1.3 "Designated Record Set" shall mean, that group of records maintained by or for Business Associate that is used, in whole or part, to make decisions about individuals, or that is Business Associate's medical and billing records about individuals as set forth in 45 C.F.R § 164.501.

1.3 "Electronic Protected Health Information" shall mean PHI that is transmitted or maintained in Electronic Media.

1.4 "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended and supplemented by the HITECH Act and its implementing regulations, as each is amended from time to time.

1.5 "HIPAA Breach Notification Rule" shall mean the federal breach notification regulations, as amended from time to time, issued under HIPAA and set forth in 45 C.F.R. Part 164 (Subpart D).

1.6 "HIPAA Privacy Rule" shall mean the federal privacy regulations, as amended from time to time, issued under HIPAA and set forth in 45 C.F.R. Parts 160 and 164 (Subparts A & E).

1.7 "HIPAA Security Rule" shall mean the federal security regulations, as amended from time to time, issued under HIPAA and set forth in 45 C.F.R. Parts 160 and 164 (Subparts A & C).

1.8 "HITECH Act" shall mean Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 17921-17954, and all its implementing regulations, when and as each is effective and compliance is required.

1.9 "Protected Health Information" or "PHI" shall mean Protected Health Information, as defined in 45 CFR § 160.103, and is limited to the PHI received, maintained, created or transmitted on behalf of, Business Associate by Subcontractor in performance of the Underlying Services.

1.10 "Underlying Services" shall mean, to the extent and only to the extent they involve the creation, maintenance, use, disclosure or transmission of PHI, the services performed by Subcontractor for Business Associate pursuant to the Underlying Services Agreement.

1.11 "Underlying Services Agreement" shall mean the written agreement(s) (other than this Agreement) by and between the Parties pursuant to which Subcontractor receives, maintains, creates or transmits

PHI for or on behalf of Business Associate in connection with the provision of the services described in that agreement(s) by Subcontractor to Business Associate or in performance of Subcontractor's obligations under such agreement(s).

## 2. Permitted and Required Uses and Disclosures of PHI by Subcontractor

2.1 Subcontractor may use or disclose PHI solely (i) as necessary to provide the Underlying Services to Business Associate and in compliance with each applicable requirement of 45 CFR § 164.504(e), (ii) as required by law, (iii) as requested by Business Associate, or (iv) as otherwise expressly authorized under this Agreement. Subcontractor shall not use or disclose PHI for any other purpose or in any other manner.

2.2 Subcontractor may, if necessary, use or disclose PHI for the proper management and administration of Subcontractor or to carry out the legal responsibilities of Subcontractor; provided, that (i) any disclosure is required by law, or (ii) Subcontractor obtains reasonable advance written assurances from the person or party to whom the PHI is disclosed that (a) the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person or party, and (b) the person or party promptly notifies Subcontractor of any instances of which it is aware in which the confidentiality of the information has been breached.

2.3 Subcontractor may create a Limited Data Set for the purpose of providing the services in accordance with the Underlying Services Agreement, provided that Subcontractor complies with its obligations under this Agreement.

2.4 Subcontractor may de-identify PHI in accordance with the requirements of HIPAA; provided that all identifiers are destroyed in accordance with this Agreement.

2.5 Subcontractor may use PHI to provide Data Aggregation services to Business Associate as permitted by the Regulations.

## 3. Obligations of Subcontractor

3.1 Subcontractor shall use appropriate safeguards, and, comply, where applicable, with the HIPAA Security Rule with respect to Electronic Protected Health Information, to prevent use or disclosure of the information other than as provided for by this Agreement.

3.2 Subcontractor shall mitigate any harmful effect of a use or disclosure of PHI by Subcontractor in violation of the requirements of this Agreement.

3.3 Subcontractor shall promptly report to Business Associate: (i) any use or disclosure of PHI not provided for by this Agreement of which it becomes aware in accordance with 45 CFR § 164.504(e)(2)(ii)(C); and/or (ii) any successful Security Incident of which Subcontractor becomes aware in accordance with 45 CFR § 164.314(a)(2)(i)(C). The parties acknowledge and agree that this section constitutes notice by Subcontractor to Business Associate of the ongoing existence and occurrence of attempted but unsuccessful Security Incidents of which no additional notice to Business Associate shall be required. Unsuccessful Security Incidents shall include, but not be limited to, pings and other broadcast attacks on Subcontractor'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 PHI.

3.4 Subcontractor shall notify the Business Associate within ten (10) days after Subcontractor's Discovery of any incident that involves an unauthorized acquisition, access, use, or disclosure of PHI. Subcontractor agrees that such notification will meet the requirements of the HIPAA Breach Notification Rule set forth in 45 CFR § 164.410. Subcontractor shall provide to the Business Associate the following information: (i) the names and contact information of all individuals whose PHI was or is believed to have been involved; (ii) a description of the nature of the incident including the types of PHI that were involved,

the date of the incident and the date of discovery; (iii) the identity of the person who made and who received (if known) the unauthorized acquisition, access and use or disclosure; (iv) a description of what the Subcontractor is doing to mitigate the damages and protect against future incidents; and (v) all other information reasonably requested by the Business Associate to enable the Business Associate to perform and document a risk assessment in accordance with the HIPAA Breach Notification Rule with respect to the incident to determine whether a Breach occurred, and all other information reasonably necessary to provide notice to Individuals, the Department of Health and Human Services and/or the media in accordance with the HIPAA Breach Notification Rule, or to any other persons to whom similar notice must be provided under any applicable State law. In the event of an incident that is required to be reported under this Section 3.4, Business Associate shall elect in its sole discretion whether Business Associate, or a third party, as agreed to by Business Associate, shall be responsible for conducting an investigation of that incident and providing any required notices as set forth in this Section 3.4. In accordance with this election, and notwithstanding anything to the contrary in this Agreement, and without limiting in any way any other remedy available to Business Associate at law, equity or contract, including but not limited to under Section 5.1 of this Agreement, Subcontractor shall (i) conduct, or pay the reasonable out-of-pocket costs of conducting, an investigation of any incident required to be reported under this Section 3.4, (ii) reimburse and pay Business Associate for all reasonable out-of-pocket expenses and costs incurred by Business Associate that arise from an investigation of any incident required to be reported under this Section 3.4, and (iii) pay the reasonable out-of-pocket costs of providing, the required notices as set forth in this Section 3.4.

3.5 Subcontractor agrees to establish procedures to investigate the incident, mitigate losses, and protect against future incidents, and to provide a description of these procedures to Business Associate within ten (10) days of receipt of a request by Business Associate. At a minimum, the established procedures implemented by Subcontractor will include the following factors when investigating the incident: (i) the nature and extent of PHI involved, including the types of identities and the likelihood data could be re-identified; (2) the unauthorized person who used the PHI (if known) or to where the disclosure was made; (3) whether PHI was actually acquired, used or disclosed in the incident; and (4) the extent to which the incident has been mitigated.

3.6 In accordance with 45 CFR § 164.502(e)(1)(ii) and 45 CFR § 164.308(b)(2), Subcontractor shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Subcontractor, agree to restrictions and conditions no less stringent than the restriction and conditions, in writing, that apply through this Agreement to Subcontractor with respect to such PHI, including but not limited to the extent that subcontractors create, receive, maintain, or transmit Electronic Protected Health Information on behalf of the Subcontractor, it shall require the subcontractors to comply with the HIPAA Security Rule.

3.7 To the extent Subcontractor is engaged to carry out Business Associate's obligations under the HIPAA Privacy Rule, Subcontractor shall comply with the requirements of the HIPAA Privacy Rule that apply to Business Associate in the performance of such obligations.

3.8 Subcontractor shall provide access to Business Associate, no later than fifteen (15) days after receipt of a request from Business Associate, to PHI in a Designated Record Set, all in accordance with the requirements under 45 CFR § 164.524.

3.9 Subcontractor shall make available and make any amendment(s) to PHI in a Designated Record Set within fifteen (15) days after receipt of a request from Business Associate, all in accordance with the requirements of 45 CFR § 164.526.

3.10 Subcontractor shall document disclosures of PHI made by Subcontractor and information related to such disclosures which are not excepted from disclosure accounting requirements under HIPAA as would be required for Business Associate to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528 and, as of the date that compliance is required by final regulations, 42 U.S.C. § 17935(c).

3.11 Subcontractor shall make available to Business Associate, within fifteen (15) days after receipt of a request, information collected in accordance with Section 3.10 of this Agreement to permit Business Associate to respond to a request by an Individual for an accounting of disclosures of PHI, all in accordance with 45 CFR § 164.528 and, as of the date compliance is required by final regulations, 42 U.S.C. § 17935(c).

3.12 Subcontractor shall notify Business Associate in writing within three (3) days after Subcontractor's receipt directly from an Individual of any request for access to or amendment of PHI, or an accounting of disclosures, as contemplated in Sections 3.7, 3.8, 3.9, and 3.10 of this Agreement.

3.13 Subcontractor agrees to make its internal practices, books, and records, including policies and procedures relating to the use and disclosure of PHI received from, or created or received by Subcontractor on behalf of, Business Associate, available to the Business Associate or to the Secretary, for purposes of the Secretary determining Business Associate's compliance with HIPAA.

3.14 Subcontractor shall not directly or indirectly receive remuneration in exchange for any PHI as prohibited by 45 CFR § 164.502(a)(5)(ii).

3.15 Subcontractor shall not make or cause to be made any communication about a product or service that is prohibited by 45 CFR §§ 164.501 and 164.508(a)(3).

3.16 Subcontractor shall not make or cause to be made any written fundraising communication that is prohibited 45 CFR § 164.514(f).

3.17 Subcontractor shall take all necessary steps, at the request of Business Associate, to comply with requests by Individuals not to send PHI to a Health Plan in accordance with 45 CFR § 164.522(a).

3.18 Subcontractor shall exercise reasonable diligence to ensure that its employees' actions or omissions do not cause Subcontractor to breach the terms of this Agreement or violate provisions of HIPAA that apply to Subcontractor.

#### 4. Minimum Necessary

Subcontractor must limit any use, disclosure, or request for use of disclosure to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of HIPAA. Subcontractor represents that all uses, disclosures, and requests it will make shall be the minimum necessary in accordance with HIPAA, Business Associate may, pursuant to HIPAA, reasonably rely on any requested disclosure as the minimum necessary for the stated purpose when the information is requested by Subcontractor. Subcontractor acknowledges that Subcontractor is also a Business Associate, as defined by HIPAA, Subcontractor is required, independent of Subcontractor's obligations under this Agreement, to comply with the HIPAA minimum necessary requirements when making any request for PHI from Business Associate.

#### 5. Term and Termination

5.1 The term of this Agreement shall commence as of the Effective Date and shall terminate when all of the PHI provided by Business Associate to Subcontractor, or created or received by Subcontractor on behalf of Business Associate, is destroyed or returned to Business Associate, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions of this Section 5.

5.2 Notwithstanding anything in this Agreement to the contrary, if Business Associate knows of a pattern of activity or practice of Subcontractor that constitutes a material breach or violation of this Agreement, then Business Associate shall provide written notice of the breach or violation to Subcontractor that specifies the nature of the breach or violation. Subcontractor must cure the breach or end the violation on or before thirty (30) days after receipt of the written notice. In the absence of a cure reasonably

satisfactory to Business Associate within the specified timeframe, or in the event the breach is reasonably incapable of cure, then Business Associate may terminate this Agreement.

5.3 Within thirty (30) days after termination or expiration of this Agreement, Subcontractor will return or destroy, if feasible, all PHI received from or created or received by Subcontractor, including all PHI in possession of Subcontractor's agents or subcontractors, on behalf of Business Associate that Subcontractor still maintains in any form, and will retain no copies of such information. To the extent return or destruction of the PHI is not feasible, Subcontractor shall notify Business Associate in writing of the reasons that return or destruction is not feasible and, if Business Associate agrees, may retain the PHI subject to this Section 5.3. Under any circumstances, Subcontractor shall extend any and all protections, limitations and restrictions contained in this Agreement to Subcontractor's use and/or disclosure of any PHI retained after the expiration or termination of this Agreement, and shall limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible. Business Associate hereby acknowledges and agrees that infeasibility includes Subcontractor's need to retain PHI for purposes of complying with its work product documentation standards and that for such retention no further notice to, or agreement by, Business Associate is required.

## 6. Miscellaneous

6.1 Each Party hereunder (the "Indemnifying Party") shall defend, hold harmless and indemnify the other Party (the "Indemnified Party") and its directors, officers, and employees against all expenses, liabilities, damages, costs, fines, penalties and losses (including reasonable attorneys' and consultant fees) (collectively, "Losses") for any third party claims brought against the Indemnified Party to the extent related to or arising from any Breach of this Agreement by the Indemnifying Party, its agents, representatives or Subcontractors. In the event of an indemnifiable claim, the Indemnified Party shall promptly notify in writing and tender its defense to the Indemnifying Party, in which case the Indemnifying Party shall provide qualified attorneys, consultants, and other appropriate professionals to represent the Indemnified Party's interests at the Indemnifying Party's expense. The Indemnified Party, at its own expense, shall have the right to participate in the defense of any such claim through counsel of its choosing. The Indemnifying Party has the sole right and discretion to settle, compromise or otherwise resolve any and all such indemnifiable claims or causes of actions. The Indemnifying Party shall not enter into any settlement without the written consent of the Indemnified Party, which consent shall not be unreasonably withheld. This Section 6.1 shall survive the expiration or termination of this Agreement for any reason.

6.2 The Parties to this Agreement do not intend to create any rights in any third parties. The obligations of Subcontractor under this Section and Section 5.3 of 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 Subcontractor, its agents, employees, contractors, successors, and assigns as set forth herein.

6.3 This Agreement may be amended or modified only in a writing signed by the Parties. No Party may assign its respective 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 purposes of effecting the provisions of this Agreement and any other agreements between the Parties evidencing their business relationship. Neither Subcontractor nor Business Associate will have the power to bind the other or incur obligations on the other Party's behalf without the other Party's prior written consent, except as otherwise expressly provided in this Agreement.

6.4 This Agreement shall be governed by the laws of the Commonwealth of Pennsylvania, without resort to the conflict of law provisions.

6.5 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 it prohibit enforcement of any obligation on any other occasion.

6.6 The Parties agree that, in the event that any documentation of the arrangements pursuant to which Subcontractor provides Underlying Services to Business Associate contains provisions relating to the use or disclosure of PHI which are more restrictive than the provisions of this Agreement, the provisions of this Agreement will control. The provisions of this Agreement are intended to establish the minimum requirements regarding Subcontractor's use and disclosure of PHI. This Agreement, together with the Underlying Services Agreements, constitute the entire agreement of the Parties relating to Subcontractor's use or disclosure of PHI and supersedes all prior agreements, oral or written, and all other communications between the Parties hereto relating to such use or disclosure.

6.7 A reference in this Agreement to a section in HIPAA means the section as in effect or as amended, and for which compliance is required. To the extent that the terms of this Agreement are unclear, they shall be construed to allow for compliance by the Parties with HIPAA and the HITECH Act. 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, the Parties agree to take such action as is necessary to amend this Agreement to ensure compliance with the requirements of HIPAA and any other applicable law.

6.8 Subcontractor understands and agrees that it will not assign, delegate, or subcontract any of its rights or obligations under this Agreement to individuals or entities residing outside the United States.

6.9 This Agreement may be executed in counterparts, each of which will constitute an original and all of which will be one and same document.

6.10 All notices, demands and requests required to be given or which may be given shall be in writing and shall be deemed to have been properly given (i) if delivered personally, on the date of such delivery, (ii) if sent by United States registered or certified mail, return receipt requested, postage prepaid, three (3) days after such notice is sent as evidenced by such receipt, or (iii) upon delivery by Federal Express or similar overnight courier service which provides evidence of delivery, on the date of delivery as so evidenced, if addressed as follows:

If to WellSpan Health:

Kathryn Magar, HIPAA Security Officer  
WellSpan Health  
140 N. Duke St.  
York, PA 17401

With a copy to:

Timothy D. Norton, II, Assistant General Counsel  
WellSpan Health  
Bruce M. Bartels Management and Governance Center  
45 Monument Road, Suite 200  
York, PA 17403

If to Subcontractor:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

PRE-APPROVED 05/09/17  
kmagar01