

BUSINESS ASSOCIATE AGREEMENT

This Agreement is made this 14th day of September, 2017 by and between the plan administrator of the covered entity, namely the W.L. Gore & Associates, Inc. Health and Welfare Plan (the "CE") and the business associate of the CE, namely Floyd Staff Consulting (the "BA"). Except as otherwise stated herein or required by law, this Agreement shall be effective as the date listed above.

I. Background

Under the Standards for Privacy, Security, Breach Notification and Enforcement Rules prescribed at 45 CFR Part 160 and 164 (the "HIPAA Rules"), in order for CE to disclose protected health information as defined in 45 CFR § 164.501 ("PHI") to BA to permit it to perform certain functions for or on behalf of CE as set forth in the administrative services agreement between the parties (the "Services Agreement"), CE must obtain an agreement with BA that it will adhere to certain guidelines designed to protect PHI. This Agreement is intended to fulfill CE's obligations with respect to BA under the HIPAA Rules and will be interpreted in a manner consistent with that intent.

II. Definitions

Initially capitalized words and phrases not otherwise defined in this Agreement will have the same definition that is given to those words and phrases under the HIPAA Rules.

III. Obligations and Activities of BA

- a. BA agrees not to use or to disclose PHI other than as permitted or required by this Agreement or as Required by Law.
- b. BA agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement or as Required by Law.
- c. BA agrees to mitigate, to the extent practicable, any harmful effect that is known to BA of a use or disclosure of PHI by BA in violation of the requirements of this Agreement.
- d. Subject to Section VII(d) below, BA agrees to report to CE any use or disclosure of PHI not provided for by this Agreement of which it becomes aware within a reasonable period of time after discovery.
- e. BA agrees to ensure that any agent, including a subcontractor, to whom it provides PHI agrees in writing, by executing a business associate agreement that is substantially similar to this Agreement, to the same restrictions and conditions that apply through this Agreement to BA with respect to such information.

- f. BA agrees to provide access, at the request of CE, to PHI in a Designated Record Set, to CE or, as directed by CE, to an Individual in order to meet the requirements under 45 CFR § 164.524. If BA maintains an Electronic Health Record, BA shall provide such information in electronic format in the manner required under the HIPAA Rules. Thus, if the requested PHI is maintained electronically, and the Individual requests an electronic copy, CE must provide the PHI in the electronic form and format requested by the Individual if the PHI is readily producible in that form and format. If the PHI is not readily producible in the requested form and format, CE must provide the PHI in a readable electronic form and format that is acceptable to the Individual. Finally, under the final regulations, if an Individual requests that his or her PHI be provided directly to another person, CE must comply with the request if the request is in writing, signed by the Individual, and identifies the designated person and where to send the PHI.
- g. BA agrees to make any amendments to PHI in a Designated Record Set that the CE directs or agrees to pursuant to 45 CFR § 164.526 at the request of CE or an Individual.
- h. BA agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by BA on behalf of CE available to the CE, or to the Secretary of the U.S. Department of Health and Human Services or designated by the Secretary, for purposes of the Secretary determining CE's compliance with the HIPAA Rules. To the extent CE determines that an examination is necessary to comply with CE's legal obligations pursuant to HIPAA relating to its privacy or security practices, CE or its authorized agents or contractors, may, at CE's expense, examine BA's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to CE the extent to which BA's privacy and security safeguards comply with the HIPAA Rules, or this Agreement.
- i. BA agrees to document such disclosures of PHI and information related to such disclosures as would be required for CE to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.
- j. BA agrees to provide to CE or an Individual, information collected in accordance with Section III(i) of this Agreement, to permit CE to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528
- k. BA shall be required to maintain a written health information privacy and security policy which meets the requirements of the HIPAA Rules and the "Security Rule" (as defined in Section VII(a) below) and shall provide a copy of such policies to CE upon request.

- l. BA shall maintain adequate insurance to protect against threatened or actual civil penalties or proceedings for violations of the HIPAA Rules.
- m. To the extent the BA is to carry out one or more of CE's obligations under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the CE in the performance of such obligations.
- n. The BA must determine whether there has been an impermissible use or disclosure of PHI under the HIPAA Rules, and must determine, and document in writing, whether the impermissible use or disclosure compromises the security or privacy of the PHI in accordance with the HIPAA Rules and Section VII(c) below. For purposes of this Agreement, "Breach" has the meaning set forth in the HIPAA Rules, including 45 CFR § 164.410. If BA determines that the incident falls under one of the exceptions to the definition of Breach contained in the HIPAA Rules, the BA must document this determination and reasons therefore in writing.
- o. Upon CE's written request, BA shall provide and/or transmit, in the form and manner requested by CE, PHI (or any form or portion thereof including de-identified information, Summary Health Information or a Limited Data Set), claims data, eligibility data, and service costs to certain designated third-parties who assist in administering the CE and are authorized by the CE to receive such information ("Designated Third Parties") for the purpose of carrying out of CE administration functions, or for such other purpose as permitted by the Privacy Rule. Electronic transmission of information by BA pursuant to this provision shall be made by a methodology which complies with the Security Rule and this Agreement.
 1. Designated Third Parties include, but are not limited to, third-party administrators, consultants, brokers, auditors, successor administrators or insurers, and stop-loss carriers, and/or data warehouse vendors, and data analytics and/or data integration vendors. CE shall enter into and maintain an appropriate business associate agreement with each Designated Third Party.
 2. BA shall provide the information and services required under this Section (III)(o) at no additional charge to CE or to its Designated Third Party.
 3. The provisions of this Section (III)(o) shall supersede any contrary or inconsistent provisions contained in the Services Agreement or any other agreement between the parties.

IV. Permitted Uses and Disclosures by BA

- a. Except as otherwise limited in this Agreement, BA may use or disclose PHI to perform functions, activities, or services for, or on behalf of, CE as specified in

the Services Agreement. If BA discloses PHI to a third party as permitted under this Agreement for reasons other than payment or treatment, BA must obtain, prior to making any such disclosure, 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.

BA (and its agents or subcontractors) shall request, use and disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure consistent with CE's minimum necessary policies. Whenever possible, BA shall only request, use and disclose a Limited Data Set (as defined in 45 CFR § 164.514(e)). BA understands and agrees that the definition of "minimum necessary" is subject to future guidance and interpretation by HHS, and shall keep itself informed of guidance issued by HHS with respect to what constitutes "minimum necessary" and abide by any such guidance.

- b. BA may use and disclose PHI as Required by Law.
- c. Except as otherwise limited in this Agreement, BA may disclose PHI for the proper management and administration of the BA, or to carry out the legal responsibilities of BA, provided that disclosures are required by law, or BA obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the BA of any instances of which it is aware in which the confidentiality of the information has been breached. Notwithstanding the above, if it is feasible for BA to use de-identified PHI for such purposes rather than PHI, BA shall be required to use such de-identified PHI.
- d. Except as otherwise limited in this Agreement, BA may use PHI to provide Data Aggregation services to CE as permitted by 45 CFR § 164.504(e)(2)(i)(B).
- e. BA may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 CFR § 164.502(j)(1).
- f. BA shall not use or disclose PHI for fundraising or marketing purposes except with the prior written consent of CE and as permitted by the HIPAA Rules.
- g. BA may use de-identified PHI to carry out any of the permissible uses or disclosures under this Agreement, or for such other purposes which relate to, and are consistent with, the provision of services to CE under the Services Agreement.

V. Obligations of CE

- a. CE shall notify BA of any limitations in its notice of privacy practices of CE in accordance with 45 CFR § 164.520, to the extent that such limitation may affect BA's use or disclosure of PHI.

- b. CE shall notify BA of any changes in, or revocation of, permission by any Individual to use or disclose PHI, to the extent that such changes may affect BA's use or disclosure of PHI.
- c. CE shall notify BA of any restriction to the use or disclosure of PHI that CE has agreed to or is required to abide by in accordance with 45 CFR § 164.522, to the extent that such restriction may affect BA's use or disclosure of PHI.

VI. Permissible Requests by CE

CE shall not request BA to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by CE, provided however that the BA may use or disclose PHI for data aggregation or management and administrative activities as provided in Sections IV(c)-(d) of this Agreement.

VII. Data Security, Breach Discovery and Notification Procedures

- a. **HIPAA Security Rule Compliance.** BA agrees to the following with respect to the Security Standards for the Protection of Electronic Protected Health Information, 45 CFR Parts 160 and 164 Subpart C (the "Security Rule"):
 - 1. to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI;
 - 2. to report, within three business days, to CE any successful or unsuccessful unauthorized attempts to access, use, disclose, modify, or destroy electronic PHI or interference with system operations in an information system containing PHI of which BA becomes aware; and
 - 3. to ensure that any agent or subcontractor to whom BA provides PHI agrees to implement safeguards to protect PHI as required by the Security Rule.
- b. **Protection of Exchanged Information in Electronic Transactions.** If BA conducts any standard transactions for or on behalf of CE, BA shall comply, and shall require any subcontractor or agent conducting such standard transactions to comply, with each applicable requirement of 45 CFR Part 162. BA shall not enter into or permit its subcontractors or agents to enter into any trading partner agreement in connection with the conduct of standard transactions for or on behalf of CE that:
 - 1. changes the definition, data condition or use of a data element or segment in a standard;

2. adds any data elements or segments to the maximum defined data set;
 3. uses any code or data elements that are either marked “not used” in the standard’s implementation specification or are not in the standard’s implementation specifications; or
 4. changes the meaning or intent of the standard’s implementation specifications.
- c. **Data Security and Discovery of Breaches.** Whenever feasible, BA shall maintain PHI in a format which will render it unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under Section 13402(h)(2) of Pub. L. 111-5. BA shall implement reasonable systems to detect and discover potential Breaches of Unsecured PHI, and shall develop procedures to notify CE in the event of a Breach of Unsecured PHI as provided in (d) below. BA shall train and educate its workforce members on its breach detection and notification policies and procedures. BA shall provide CE with all documentation relating to its investigation of breaches or potential breaches, and reasons incidents were not disclosed to CE, upon its request.
- d. **Reporting of Improper Access, Use or Disclosure.** BA shall report to CE in writing of any Breach of Unsecured PHI of which it becomes aware without unreasonable delay and in no case later than five calendar days after discovery. Such notification shall, at a minimum, contain the following information:
1. a description of the incident, including the date of the breach and the date of discovery and the PHI involved;
 2. a description of the type of unsecured PHI that was involved (e.g., name, Social Security Number, procedure, diagnosis, treatment, and so forth);
 3. a description of what the BA is doing to investigate, mitigate harm, and protect against future similar breaches; and
- e. **Notification to Individuals and the Secretary.** If the CE determines that there has been a Breach of Unsecured PHI by the BA or a subcontractor of the BA, unless directed otherwise by CE, the BA shall provide all notifications required by 45 C.F.R. 164.404, 45 C.F.R. 164.406 and 45 C.F.R. 164.408 at its own cost and expense. In addition, BA shall be responsible to provide Individuals, at its own cost and expense, with fraud and/or credit protection as BA and/or CE determines may be necessary to mitigate a Breach.

BA agrees to provide appropriate staffing and have established procedures to contact the BA for additional information regarding the breach. Such procedures may include a toll-free telephone number, an e-mail address, a posting on its Web

site and a postal address. Costs and expenses of such contact procedures will be borne by the BA.

BA agrees that, in the event of a breach, it has the burden to demonstrate that it has complied with all notifications requirements set forth above, including evidence demonstrating the necessity of a delay in notification to the CE.

- f. BA's Agents and Subcontractors. BA shall ensure that any agents, including subcontractors, to whom it provides PHI, agree in writing to the same restrictions and conditions that apply to BA as set forth above. BA shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.

VIII. Term and Termination

- a. Term. This Agreement shall terminate when all of the PHI provided by CE to BA, or created or received by BA on behalf of CE, is destroyed or returned to CE, or, if it is not feasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
- b. Termination for Cause. Upon CE's knowledge of a material breach by BA, CE shall either:
1. provide an opportunity for BA to cure the breach or end the violation and terminate this Agreement and the Services Agreement if BA does not cure the breach or end the violation within the time specified by CE; or
 2. immediately terminate this Agreement and the Services Agreement if BA has breached a material term of this Agreement and cure is not possible.
- c. Judicial or Administrative Proceedings. CE may terminate the Agreement, effective immediately, if (i) BA is named as a defendant in a criminal proceeding for a violation of the HIPAA Rules or other security or privacy laws or (ii) a finding or stipulation that the BA has violated any standard or requirement of HIPAA Rules, or other security or privacy laws is made in any administrative or civil proceeding in which the BA has been joined.
- d. Effect of Termination. Upon termination of this Agreement for any reason, BA, with respect to PHI received from CE, or created, maintained, or received by BA on behalf of CE, shall:
1. retain only that PHI which is necessary for BA to continue its proper management and administration or to carry out its legal responsibilities;
 2. return to CE (or if CE agrees, destroy) the remaining PHI that the BA still maintains in any form;

3. continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI, for as long as BA retains the PHI;
 4. not use or disclose the PHI retained by BA other than for the purposes for which such PHI was retained and subject to the same conditions set out at Section IV(c) which applied prior to termination; and
 5. return to CE (or, if agreed to by CE, destroy) the PHI retained by BA when it is no longer needed by BA for its proper management and administration or to carry out its legal responsibilities.
- e. The obligations of BA under this Section VIII shall survive the termination of this Agreement.

IX. Indemnification

The BA will indemnify and hold harmless the CE and any affiliate, officer, director, employee or agent of the CE from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any non-permitted use or disclosure of PHI, any violation of the HIPAA Rules, or other breach of this Agreement by the BA or any subcontractor, agent, person or entity under the BA's control.

X. Miscellaneous

- a. Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.
- b. Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time to permit CE to comply with the requirements of the HIPAA Rules. This Agreement may be amended only in a writing signed by each party. The parties acknowledge that amendment of Agreement may be required to provide for procedures to ensure compliance with future guidance, regulations, interpretations or modifications to HIPAA's privacy or security standards. The parties specifically agree to take such action as is necessary to implement the standards and requirements of such rules and other applicable laws relating to the security or confidentiality of PHI. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Agreement embodying written assurances consistent with the standards and requirements of the HIPAA Rules or other applicable laws. CE may terminate the Agreement upon 30 days written notice in the event (i) BA does not promptly enter into negotiations to amend the Agreement when requested by CE pursuant to this Section or (ii) BA refuses to amend the Agreement providing assurances regarding the safeguarding of PHI that CE, in its

sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.

- c. Assistance in Litigation or Administrative Proceedings. BA shall make itself and any subcontractors, employees or agents assisting BA in the performance of its obligations under the Services Agreement or this Agreement, available to CE, at no cost 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 or other laws relating to security and privacy, except where BA or its subcontractor, employee or agent is a named adverse party.
- d. Disclaimer. CE makes no warranty or representation that compliance by BA with this Agreement or the HIPAA Rules will be adequate or satisfactory for BA's own purposes. BA is solely responsible for all decisions made by BA regarding its obligations under such laws.
- e. Interpretation. The provisions of this Agreement shall prevail over any provisions in the Services Agreement that may conflict or appear inconsistent with any provision in this Agreement. This Agreement and the Services Agreement shall be interpreted as broadly as necessary to implement and comply with the HIPAA Rules. The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with such rules.
- f. Governing Law. To the extent not preempted by federal law, this Agreement shall be governed and construed in accordance with the laws of the Commonwealth of Pennsylvania other than its conflict of law provisions.
- g. Supersession. The provisions of this Agreement are intended by the parties hereto to amend and, to the extent inconsistent with, to supersede the provisions of the Services Agreement.
- h. 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.
- i. Ownership of Information. CE holds sole and exclusive ownership, right, title, and interest in and to the PHI, or any form or portion thereof including de-identified PHI, Summary Health Information or a Limited Data Set. BA does not hold and will not acquire, any right, title, or interest in or to the PHI or any portion thereof, including aggregate or de-identified PHI, Summary Health Information or a Limited Data Set, by virtue of this Agreement, the Services Agreement, or any other agreement between the parties, by virtue of providing goods or services to CE, or as a result of the selection, arrangement, creation, or processing of PHI. The provisions of this Section (X)(i) shall supersede any

contrary or inconsistent provisions contained in the Services Agreement or any other agreement between the parties. The provisions of this Section (X)(i) shall survive the termination of this Agreement.

IN WITNESS WHEREOF, and intending to be legally bound, the parties hereto have caused their authorized representatives to execute and deliver this Agreement on their behalf.

Covered Entity:

W.L. Gore & Associates, Inc. Health and Welfare Plan
By its Plan Administrator

Mandy K.S.L.
GLOBAL TOTAL REWARDS LEADER

Business Associate:

[NAME]

By: James Andrew Hogg, Sr.
Title: Managing Director