DATA PROCESSING AGREEMENT ("DPA")

INSTRUCTIONS FOR CHS INC. ("CHS") VENDORS

WHO SHOULD EXECUTE THIS DATA PROCESSING AGREEMENT ("DPA"):

If you are CHS Vendor and a data processor under the GDPR, CHS requires that you enter into a data processing agreement (DPA). Our GDPR compliant DPA is attached and ready for your signature in accordance with the instructions below.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of several parts:
   a. the main body of the DPA
   b. Annex 1- Details of Data Processing
2. To complete this DPA, Vendor must populate the applicable areas and sign the DPA signature boxes as the **Processor or Data Importer.**
3. Send the completed and signed DPA to your CHS Relationship Manager.
4. If you have any questions or concerns please email your CHS Relationship Manager or privacy@chsinc.com.

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") forms part of the Agreement between CHS Inc. ("Controller") and the CHS Inc. vendor and data processor ("Processor") (the "Agreement") pursuant to which Processor will provide the Services (as defined in the Agreement) to Controller. Processor agrees to comply with the following provisions with respect to any Personal Data Processed for Controller in connection with the provision of the Services. References to the Agreement will be construed as including this DPA. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement. This DPA takes precedence over the Agreement to the extent of any conflict.

1. DEFINITIONS

In this DPA, the following terms shall have the meanings set out below:

"Affiliates" means any entity which is controlled by, controls or is in common control with Processor.

"Controller" means the Controller that has executed the Agreement for Services.

"Controller Personal Data" means any Personal Data Processed by Processor on behalf of Controller pursuant to or in connection with the Agreement.

"Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller.

"Data Protection Laws" means all laws and regulations, including laws and regulations of the European Union, applicable to the Processing of Personal Data under the Agreement.

"Data Subject" means the individual to whom Personal Data relates.

"Personal Data" means any information relating to an identified or identifiable person.

"Privacy Shield" means the EU-US Privacy Shield Framework and/or the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning).

"Security Breach" has the meaning set forth in Section 7 of this DPA.

"Sub-processor" means any Data Processor engaged by Processor.

2. PROCESSING OF CONTROLLER PERSONAL DATA

2.1 The parties agree that with regard to the Processing of Controller Personal Data, Controller is the Data Controller and Processor is the Data Processor.

2.2 Processor shall process Controller Personal Data in accordance with the requirements of the Data Protection Laws. Controller will ensure that its instructions for the Processing of Controller Personal Data shall comply with the Data Protection Laws.

2.3 During the Term of the Agreement, Processor shall only Process Controller Personal Data on behalf of and in accordance with the Agreement and Controller's instructions. Controller instructs Processor to Process Controller Personal Data for the following purposes: (i) Processing in accordance with the Agreement and any applicable orders; and (ii) Processing to comply with other reasonable instructions provided by Controller where such instructions are consistent with the terms of the Agreement.

2.4 The sole objective of Processing of Controller Personal Data by Processor is the performance of the Services pursuant to the Agreement. The types of Controller Personal Data and categories of Data Subjects Processed under this DPA are described in the attached Annex 1 entitled "Details of Processing Personal Data".

3. RIGHTS OF DATA SUBJECTS

3.1 To the extent Controller, in its use or receipt of the Services, does not have the ability to correct, amend, restrict, block or delete Controller Personal Data, as required by Data Protection Laws, Processor shall comply with requests by Controller to facilitate such actions.

3.2 Processor shall promptly but within no later than forty-eight (48) hours, notify Controller if it receives a request from a Data Subject for access to, correction, amendment, deletion of or objection to the processing of that person's Personal Data. Processor shall not respond to any such Data Subject request without Controller's prior written consent except to confirm that the request relates to Controller. Processor shall provide Controller with commercially reasonable cooperation and assistance in relation to handling of a Data Subject's request to the extent Controller does not have access to such Controller Personal Data through its use or receipt of the Services.

4. PROCESSOR PERSONNEL

4.1 Processor shall ensure that its personnel engaged in the Processing of Controller Personal Data are informed of the confidential nature of the Controller Personal Data and are subject to written obligations of confidentiality.

4.2 Processor shall ensure that access to Controller Personal Data is strictly limited to those personnel who require such access to perform the Services.

4.3 Processor will appoint a data protection officer where such appointment is required by Data Protection Laws. The appointed person may be reached by email via the email address provided by Processor on the signature page of this DPA. Processor will promptly notify Controller of any change in the data protection officer contact information

5. SUB-PROCESSORS

5.1 Processor shall give Controller prior written notice which includes email notice to privacy@chsinc.com, of the appointment of any Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. Processor shall not appoint any Sub-processor except with the prior written consent of Controller.

5.2 Controller acknowledges and agrees that (i) Processor Affiliates may be retained as Sub-processors; and (ii) Processor may engage third-party Sub-processors in connection with the provision of the Services. Any such Sub-processors will be permitted to obtain Controller Personal Data only to deliver the services Processor has retained them to provide, and are prohibited from using Controller Personal Data for any other purpose. Processor agrees that any agreement with a Sub-processor will include substantially the same data protection obligations as set out in this DPA.

5.3 With respect to each Sub-processor, Processor shall: (i) before the Sub-processor first Processes Personal Data, carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Controller Personal Data required hereunder, and (ii) provide to Controller for review such copies of the Processors' agreements with Sub-processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Controller may request from time to time.

6. SECURITY; AUDIT RIGHTS; PRIVACY IMPACT ASSESSMENTS

6.1 Processor shall implement and maintain appropriate technical and organizational measures to protect Controller Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of the Controller Personal Data and having regard to the nature of the Controller Personal Data which is to be protected. These technical and organizational measures shall include, at a minimum, all of the measures set out in the CHS Data Security Addendum which can be found at: https://www.chsinc.com/-/media/project/chs/chs-inc/files/other/chs-privacy-center/privacy-data-security-addendum-english.pdf.

6.2 Processor shall make available to Controller on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Controller or an auditor mandated by Controller in relation to the Processing of Controller Personal Data by Processor.

6.3 Processor will provide reasonable assistance to Controller where Controller is conducting a privacy impact assessment.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1 If Processor becomes aware of any unlawful access to any Controller Personal Data stored on Processor's equipment or in Processor's facilities, or access to equipment or facilities resulting in any loss, disclosure, or alteration of Controller Personal Data ("Security Breach"), Processor will provide to Controller the name and contact information for one or more representatives of Processor (which may

be a live-staffed help desk) who will serve as Controller's primary security contact and be available to assist Controller 24 hours per day, seven days per week as a contact in resolving obligations associated with any actual or suspected Security Breach.

In the case of any actual or suspected Security Breach, the following provisions will apply.

(i) Processor will immediately notify Controller of the actual or suspected Security Breach. If the agreement or other terms and conditions under which Processor provides goods, services, or software to the CHS Party provide for a specific Controller contact, Processor will notify that contact and also send an e-mail notification to CHSinformationsecurity@chsinc.com. If the agreement or other terms and conditions under which Processor provides goods, services, or software to the Controller do not provide for a specific Controller contact, Processor will notify Controller Information Security by e-mail at CHSinformationsecurity@chsinc.com and/or IT Service Center Phone: 651-355-5555 or 800-852-8185. Processor will also provide to Controller any other notice required by law.

(ii) Immediately following Processor's notification to Controller of an actual or suspected Security Breach, Processor will coordinate with the Controller and its designees to investigate the actual or suspected Security Breach. Processor will reasonably cooperate with the Controller in the Controller's handling of the matter, including, without limitation: (A) assisting with any investigation; (B) providing Controller with physical access to the facilities and operations affected; (C) facilitating interviews with Processor's employees and others involved in the matter; and (D) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by the Controller or its designees.

(iii) Processor will, at its own expense, immediately contain and remedy any Security Breach, including, but not limited to, taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards. Processor shall reimburse Controller and its Affiliates for all costs incurred by Controller in responding to, and mitigating damages caused by, any Security Breach, including, but not limited to, all costs of notice and/or remediation.

(iv) Except as is required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, Processor will not inform any third party of any Security Breach without first obtaining Controller's prior written consent. Where Processor informs any third party of a Security Breach as required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, Processor will give notice to the Controller concurrently with such other notice.

(v) Except as is required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, Controller will have the sole right to determine: (A) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by law or regulation, or otherwise, in Controller's discretion; and (B) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

(vi) Processor will maintain and preserve all documents, records, and other data related to any Security Breach.

8. RETURN AND DELETION OF CONTROLLER DATA

8.1 Return or other Provision of Personal Data. At the termination or completion of services in connection with which Supplier holds Personal Data, Processor will, at Controller's option and upon request made by Controller within 30 days after such termination or completion, provide to Controller, in industry-standard electronic form, such Personal Data as Processor holds as of the time immediately before termination or completion. If the relevant agreement associated with such services does not provide for compensation for such provision of Personal Data and does not require provision of such Personal Data at no charge to Controller, Controller will pay to Processor the actual cost of media and personnel necessary to provide the Personal Data as required by in this section.

8.2 Deletion and Destruction of Personal Data. If and when Processor is required to destroy Personal Data, Processor will destroy such Personal Data using methods at least as complete and reliable as those contained in NIST Special Publication 800-88, as amended, or its successor document. Where Processor is permitted to retain Personal Data in de-identified or anonymized form, Processor will de-identify and anonymize the Personal Data according to NISTIR 8053, as amended, or its successor document or, where required by law, as provided for under such law.

9 STANDARD CONTRACTUAL CLAUSES

Controller (as "data exporter") and Processor (as "data importer") will hereby enter into the Standard Contractual Clauses in respect of any transfer of Controller Personal Data from Controller to Processor which can be found at: https:// www.chsinc.com/-/media/project/chs/chs-inc/files/other/chs-privacy-center/controller-processor-standard-contractual-cla.pdf.

10. INDEMNIFICATION

Except for any indirect, special, incidental, exemplary, punitive, or consequential damages, the Processor shall indemnify, defend and hold harmless Controller and its affiliates and their officers, directors, employees and agents from and against any and all claims, demands, causes of action, damages, liabilities, fines, penalties and expenses (including, without limitation, expenses of investigation, settlement, litigation and attorney's fees and costs incurred in connection therewith) arising out of or resulting from: (i) any breach of this DPA by the Processor or its employees, agents or Sub-processors; or (ii) the negligence or willful misconduct of the Processor or its employees, agents or Sub-processors. This indemnification obligation will survive the expiration of the Agreement or any SOW.

11. PARTIES TO THIS DPA

Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

12. LEGAL EFFECT

This DPA shall only become legally binding between Controller and Processor when signed by both parties. If this document has been electronically signed by either party such signature will have the same legal affect as a hand-written signature.

Agreed for and on behalf of Processor

Signed: _____

Name: _____

Title: _____

Date: _____

Processor Data Protection Officer Contact Information, if applicable

Name: _____

Email Address: _____

Phone Number: _____

Agreed for and on behalf of CHS Inc.

Signed: _____

Name: _____

Title: _____

Date: _____

ANNEX 1

DETAILS OF PROCESSING PERSONAL DATA

This Annex 1 includes certain details of the Processing of Controller (CHS Inc.) Personal Data as required by Article 28(3) of the GDPR (or as applicable, equivalent provisions of any other Data Protection Law).

Subject Matter and Duration of the Processing of Controller Personal Data (Check One):

- □ The subject matter and duration of the Processing of the Controller Personal Data are set out in the Agreement and DPA, including any Annex, Appendix or Schedule to the DPA.

- □ If not named in the Agreement or DPA, please fill in the subject matter and duration here:

The Nature and Purpose of the Processing of Controller Personal Data:

Nature (Check all that apply):

- □ Collection
- □ Recording
- □ Disclosure
- □ Deletion
- □ Alteration
- □ Restriction
- □ Use
- □ Storage
- □ Profiling or other automated decision-making
- □ Other (please specify): _____

Purpose (Choose One):

- □ Controller Personal Data is used to provide good or services as set out in the Agreement.

- □ If not named in the Agreement, please fill in the purpose here: _____

Types of Personal Data Processed (Check all that apply):

- □ Identification and contact data (name, address, telephone, email address, personal identification number etc.)
- □ Electronical localization and identification data (GPS, mobile phone, IP addresses and cookies etc.)
- □ Financial specifications (income, transactions, credit information, taxation information etc.)
- □ Human resources data
- □ Physical data (size, weight, height etc.)
- □ Psychological data (personality, character etc.)
- □ Consumer interests, leisure, behavior and habits
- □ Education, training
- □ Profession and position/role
- □ Image, video and/or sound recordings or streaming
- □ Personal characteristics (age, gender, marital status, family composition, etc.)
- □ Memberships
- □ Household and residential related data and features
- □ Property information (vehicle owner, real property owner etc.)
- □ Legal information (judgments, court- and authority decisions etc.)
- □ Other types of Personal Data: ___

List Specific Data Elements Processed: _____

Types of Sensitive Personal Data Processed (Check all that apply):

- □ Genetic data
- □ Biometric data (facial images, finger prints etc.)
- □ Health data
- □ Racial or ethnic data
- □ Political opinions
- □ Religious or philosophical beliefs
- □ Trade union membership

□ Sex life or sexual orientation data

□ Criminal convictions and offences data

Categories of Data Subjects whose Personal Data is Processed (Check all that apply):

□ CHS employees, consultants and representatives

□ Customers

□ Consumers

□ Suppliers

□ Children

□ Other, please fill in category here: _____

The Obligations and Rights of the Controller and Controller Affiliates (Choose One):

□ The obligations and rights of Controller and Controller Affiliates are set out in the Agreement and the DPA, including any Annex, Appendix or Schedule to the DPA.

□ If the obligations and rights of Controller and Controller Affiliates are set out elsewhere or in any other agreement, then please specify here: _____