Effective December 12, 2022. This Data Processing Agreement supersedes and replaces all prior versions.

Data Processing Agreement

This Data Processing Agreement (the "Agreement") between Provider (sometimes referred to as "Provider," "we," "us," or "our"), and the Client found on the applicable Master Services Agreement, Order, or Service Description (sometimes referred to as "you," or "your,") and, together with the Order, Proposal, Master Services Agreement, and other relevant Service Attachments or Descriptions, forms the Agreement between the parties the terms to which the parties agree to be bound.

The parties agree as follows:

1. Health Insurance Portability and Accountability Act ("HIPAA") Data Processing. This Agreement documents the safeguards imposed upon the parties to protect health information that is subject to the Health Insurance Portability and Accountability Act ("HIPAA"). If Provider is engaged as a "Business Associate" under HIPAA, then this Agreement shall apply to Provider's activities as a Business Associate. If HIPAA applies to Provider's activities as a Business Associate, in Order to demonstrate the parties' compliance with HIPAA, this Agreement applies to each agreement between Provider or any of Provider's Affiliates and Client or any of Client's Affiliates under which Provider engages protected health information as part of its performance.

a. DEFINITIONS

The following terms used in this Agreement have the same meanings as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions:

- Business Associate. "Business Associate" generally has the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this Agreement, means Provider.
- Covered Entity. "Covered Entity" generally has the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this Agreement, means Client.
- HIPAA Rules. "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

b. OBLIGATIONS OF BUSINESS ASSOCIATE

Business Associate agrees to:

i. Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

ii. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;
iii. Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;
iv. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;
v. Make available protected health information in a designated record set to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.524;
vi. Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;
vii. To the extent required by regulators, maintain and make available the information required to provide an accounting of disclosures to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.528;
viii. To the extent the Business Associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and
ix. To the extent required by regulators, make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

c. PERMITTED USES AND DISCLOSURES

i. Business Associate may only use or disclose protected health information as necessary to perform the services set forth in the Master Services Agreement. The Business Associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the Business Associate will de-identify the information and the permitted uses and disclosures by the Business Associate of the de-identified information.
ii. Business Associate may use or disclose protected health information as required by law.
iii. Business Associate agrees to make uses and disclosures and requests for protected health information consistent with the covered entity's minimum necessary policies and procedures.
iv. Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by a covered entity.
v. Business Associate may disclose protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
vi. Business Associate may provide data aggregation services relating to the health care operations of the covered entity.

d. PRIVACY PRACTICES AND RESTRICTIONS

i. Covered entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.
ii. Covered entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect Business Associate's use or disclosure of protected health information.
iii. Covered entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

e. PERMISSIBLE REQUESTS

Covered entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity.

2. General Data Protection Regulation ("GDPR")

The European General Data Protection Regulation ("GDPR") imposes specific obligations on "Processors", "Controllers", and others with regard to their vendor relationships (as defined below). GDPR requires companies to conduct appropriate due diligence on processors and to have contracts containing specific provisions relating to data protection.

If Provider is engaged in "Processing" of data, then this Addendum shall apply to Provider's activities as a "Processor". If GDPR applies to Provider's activities as a Processor, in order to demonstrate the parties' compliance with GDPR, this Addendum applies to each agreement between Provider and Client under which Provider Processes Personal Data as part of performing under that agreement ("Agreement"). If GDPR is applicable to Provider's activities, the Addendum will be effective on the last signature date set forth below ("Addendum Effective Date").

DEFINITIONS

"GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation, together with any addition implementing legislation, rules or regulations that are issued by applicable supervisory authorities. All capitalized terms in this Addendum which are not otherwise defined in this Addendum or in the Agreement have the meaning set forth in the GDPR. Words and phrases in this Addendum shall, to the greatest extent possible, have the meanings given to them in Article 4 of the GDPR. In particular:

(a) "Controller" has the meaning given to it in Article 4(7) of the GDPR: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law," but only to the extent such personal data pertains to residents of the European Economic Area ("EEA") or are otherwise subject to the GDPR.

(b) "Personal Data" has the meaning given to it in Article 4(1) of the GDPR: "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person," but only to the extent such personal data pertains to residents of the EEA or are otherwise subject to the GDPR.

(c) "Personal Data Breach" has the meaning given to it in Article 4(12) of the GDPR: "[any] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access

to, personal data transmitted, stored or otherwise processed."

(d) "Processing" has the meaning given to it in Article 4(2) of the GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"

(e) "Processor" has the meaning given to it in Article 4(8) of the GDPR: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller," but only to the extent such personal data pertains to residents of the EEA or are otherwise subject to the GDPR.

(f) "Sub-processor" means any processor as defined in Article 4(8) of the GDPR: "[any] natural or legal person, public authority, agency or other body which processes personal data" on behalf of the Processor (including any affiliate of the Processor).

(g) "Transfer" means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Sub-processor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.

OBLIGATIONS OF A PROCESSOR

Technical Measures

In accordance with GDPR Article 28(1), Processor represents that it has implemented appropriate technical and organizational measures in such a manner that its Processing of Personal Data will meet the requirements of GDPR and ensure the protection of the rights of the data subjects.

Sub-processors

In accordance with GDPR Article 28(2), the Processor shall not engage any Sub-processor without prior specific or general written authorization of Client. In the case of general written authorization, the Processor shall inform Client of any intended changes concerning the addition or replacement of other Sub-processors and give Client the opportunity to object to such changes. The Processor shall also comply with the requirements for sub-processing as set forth in Article 28(4), namely that the data protection obligations set forth herein (and as may otherwise be agreed by the Processor in the Agreement) such be imposed upon the Sub-processor, so that the Processor's contract with the Sub-processor contains sufficient guarantees that the Processing will meet the requirements of GDPR.

Processing & Security

In accordance with GDPR Article 28(3), the following terms are incorporated by reference into the Agreement:

(a) The Processor shall only process the Personal Data only (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from Client, including with regard to any Transfers, and (iii) as needed to comply with law (in which case, the Processor shall provide prior notice to Client of such legal requirement, unless that law prohibits this disclosure), and (iv) with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by European Union or Member State law to which Client is subject, in such case, Client will inform Provider of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(b) Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) Processor shall take all security measures required by GDPR Article 32, namely:

(i) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(ii) In assessing the appropriate level of security account shall be taken in particular of the risks that are p resented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

(iii) The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process them except on instructions from Client, unless he or she is required to do so by EEA Member State law.

(d) Taking into account the nature of the processing, Processor shall reasonably assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Client's obligation to respond to requests for exercising the data subject's rights;

(e) Taking into account the nature of processing and the information available to the Processor, Processor shall comply with (and shall reasonably assist Client to comply with) the obligations regarding Personal Data Breaches (as set forth in GDPR Articles 33 and 34), data protection impact assessments (as set forth in GDPR Article 35), and prior consultation (as set forth in GDPR Article 36);

(f) At Client's discretion, the Processor shall delete or return all the Personal Data to Client after the end of the provision of Services relating to Processing, and delete existing copies unless applicable EEA member state law requires storage of the Personal Data;

(g) The Processor shall provide Client with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client; and

(h) The Processor shall immediately inform Client if, in its opinion, an instruction infringes the GDPR other EEA Member State data protection provisions.

Personal Data Transfers

The Processor shall not Transfer any Personal Data (and shall not permit its Sub-processors to Transfer any Personal Data) without the prior consent of the Client. The Processor understands that Client must approve and document that adequate protection for the Personal Data will exist after the Transfer, using contracts that provide sufficient guarantees (such as standard contractual clauses) unless another legal basis for the Transfer exists.

Unauthorized Access & Breach Notification

The Processor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Processor will notify Client without undue delay in the event of any Personal Data Breach.

Maintenance & Availability of Records

The Processor shall maintain all records required by Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for Client) Processor shall make them available to Client upon request.

COMPLIANCE WITH LAWS

To the extent that GDPR applies to Provider and Client's activities under this Attachment, Provider shall comply with all data protection laws applicable to Provider in its role as a data Processor Processing Personal Data. For the avoidance of doubt, Provider is not responsible for complying with data protection laws applicable to Customer (as a data Controller) or Customer's industry. Customer shall comply with all data protection laws applicable to Customer as a data Controller.

If Provider maintains Personal Data on Provider's computers or machines, Provider will take responsibility to assist Customer with GDPR compliance at Provider's then current hourly rates.
If Customer maintains data on Customer's computers or machines, and not on Provider's machines or computers, Provider will assist Customer with GDPR compliance at Provider's then current hourly rates.

DEFENSE OF CLAIMS

Where Provider faces an actual or potential claim arising out of or related to violation of any GDPR obligations

(e.g., Article 82 of the GDPR) concerning the Services, Client will promptly provide all materials and information requested by Provider that is relevant to the defense of such claim and the underlying circumstances concerning the claim.

STATEMENT OF WORK

The subject matter and duration of the Processing, the nature and purpose of the Processing, and the type of Personal Data and categories of data subjects will be described in a statement of work, purchase order or written agreement signed by the parties' authorized representatives, which forms an integral part of the Agreement.

INSURANCE

In addition to any other insurance required under the Agreement, Client will maintain insurance coverage for privacy and cybersecurity liability (including costs arising from data destruction, hacking or intentional breaches, crisis management activity related to data breaches, and legal claims for security breach, privacy violations, and notification costs) of at least $2,000,000 US per occurrence.

TERM AND TERMINATION

(a) Term. The Term of this Agreement shall be effective as of the date signed by both parties below, and shall terminate upon the termination of the Agreement or upon the date Client terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Provider authorizes termination of this Agreement by Client, if Client determines Provider has violated a material term of the Agreement and Provider has not cured the breach or ended the violation within ten (10) business days.

(c) Effect of Termination. Upon termination of this Agreement for any reason, Provider, with respect to Personal Data received from Client, or created, maintained, or received by Provider on behalf of Client, shall:

(i) Retain only that Personal Data which is necessary for Provider to continue its proper management and administration or to carry out its legal responsibilities;

(ii) Return to Client [or, if agreed to by Client, destroy] the remaining Personal Data that the Provider still maintains in any form;

(iii) Continue to use appropriate safeguards with respect to Personal Data to prevent use or disclosure of the Personal Data, other than as provided for in this Section, for as long as Provider retains the Personal Data;

(iv) Not use or disclose the Personal Data retained by Provider other than for the purposes for which such Personal Data was retained and subject to the same conditions set forth in this Agreement; and

(v) Return to Client [or, if agreed to by Client, destroy] the Personal Data retained by Provider when it is no longer needed by Provider for its proper management and administration or to carry out its legal responsibilities.

In addition, Client's termination of this Agreement for cause constitutes good cause for Client to terminate any Service Attachments signed under the Agreement in connection with which Provider received any Personal Data from Client.

(d) Survival. The obligations of the Provider under this Section shall survive the termination of this Agreement.