DATA PRIVACY AND PROTECTION ADDENDUM

This Data Privacy and Protection Addendum (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 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 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. Gramm-Leach-Bliley Act ("GLBA") Data Processing. This section documents the safeguard standards imposed to protect Client financial information subject to the Gramm-Leach Bliley Act ("GLBA"). To the extent Provider's services constitute processing of personal information governed by GLBA, these provisions shall apply.

a. DEFINITIONS

All capitalized terms in this Addendum which are not otherwise defined in this Addendum or in the MSA have the meaning set forth in Title V of the Gramm-Leach-Bliley Act (P. L. 106-102; 15 USC §6801 et seq.) and the regulations issued pursuant thereto by the Financial Institution's Functional Regulator.

b. RECEIPT OF INFORMATION

To perform its duties under the Agreement, Provider is authorized and permitted to receive, hold and, to the extent necessary, review Nonpublic Personal Information of Client in order to provide services for Client at Client's direction as provided under the MSA. Provider may further use and disclose Nonpublic Personal Information for the proper management and administration of the business of Provider.

c. OBLIGATIONS OF SERVICE PROVIDER

Provider will take reasonable steps to:

- Implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for the security and protection of Nonpublic Personal Information and further containing each of the elements set forth in § 314.4 of the Gramm Leach Bliley Standards for Safeguarding Client Information (16 C.F.R. § 314) and the Red Flag Rules issued by the Federal Trade Commission;
- Ensure the security and confidentiality of Nonpublic Personal Information received from Client;
- Protect against any anticipated threats or hazards to the security or integrity of Nonpublic Personal Information;
- Protect against unauthorized access to or use of such information that could result in harm or inconvenience to Client;
- Ensure the proper disposal of Nonpublic Personal Information, as set forth in the MSA or in Service Attachments signed under the MSA, and
- Notify Client of any loss or breach of the security or Confidentiality of Client's Nonpublic Personal Information.

d. PERMITTED USES AND DISCLOSURES

Provider may disclose the information received by it under the Agreement only if the disclosure is required by law.

e. PERMISSIBLE REQUESTS

Client shall not request Provider to use or disclose Nonpublic Personal Information in any manner that would not be permissible Title V of the Gramm-Leach-Bliley Act (P. L. 106-102; 15 USC §6801 et seq.) and the regulations issued pursuant thereto if done by Client.

3. Department of Defense Standards for Controlled Unclassified Information ("CUI"). This section

documents the safeguards imposed to protect CUI subject to the DoD and CMMC's standards. To the extent Provider's services involve CUI subject to DoD or CMMC standards or regulations, these provisions shall apply.

a. **System Environment.** Provider will prepare a detailed description of system boundaries, system interconnectedness, and key devices.

b. **Requirements.** Provider will thoroughly describe how the CMMC requirements have been implemented for each of the following:

   i. Access Control
   ii. Awareness and Training
   iii. Audit and Accountability
   iv. Configuration Management
   v. Identification and Authentication
   vi. Incident Response
   vii. Maintenance
   viii. Media Protection
   ix. Personnel Security
   x. Physical Protection
   xi. Risk Assessment
   xii. Security Assessment
   xiii. System and Communication Protection
   xiv. System and Information Integrity

4. California Consumer and Privacy Act. This section documents the safeguard standards imposed to protect Client information subject to the California Consumer and Privacy Act ("CCPA"). To the extent Provider's services constitute processing of personal information governed by CCPA, these provisions shall apply.

a. **DEFINITIONS**
   i. "CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 et. seq., and its implementing regulations.
   ii. "Client Personal Information" means any Client Data maintained by Client and processed by Provider solely on Client's behalf, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, to the extent that such information is protected as "personal information" (or an analogous variation of such term) under applicable U.S. Data Protection Laws.
   iii. "U.S. Data Protection Laws" means all laws and regulations of the United States of America, including the CCPA, applicable to the processing of personal information (or an analogous variation of such term).
   iv. "Service Provider" has the meaning set forth in Section 1798.140(v) of the CCPA.

b. **Roles.** The parties acknowledge and agree that with regard to the processing of Client Personal Information performed solely on behalf of Client, Provider is a Service Provider and receives Client Personal Information pursuant to the business purpose of providing the Services to Client in accordance with the Agreement.

c. **No Sale of Client Personal Information to Provider**. Client and Provider hereby acknowledge and agree that in no event shall the transfer of Client Personal Information from Client to Provider pursuant to the Agreement constitute a sale of information to Provider, and that nothing in the Agreement shall be construed as providing for the sale of Client Personal Information to Provider.

d. **Limitations on Use and Disclosure**. Provider is prohibited from using or disclosing Client Personal Information for any purpose other than the specific purpose of performing the Services specified in the Agreement, the permitted business purposes set under applicable law, and as required under applicable

law. Provider hereby certifies that it understands the foregoing restriction and will comply with it in accordance with the requirements of applicable U.S. Data Protection Laws.

e. **Data Subject Access Requests**. Provider will reasonably assist Client with any data subject access, erasure or opt-out requests and objections. If Provider receives any request from data subjects, authorities, or others relating to its data processing, Provider will without undue delay inform Client and reasonably assist Client with developing a response (but Provider will not itself respond other than to confirm receipt of the request, to inform the data subject, authority or other third party that their request has been forwarded to Client, and/or to refer them to Client, except per reasonable instructions from Client). Provider will also reasonably assist Client with the resolution of any request or inquiries that Client receives from data protection authorities relating to Provider, unless Provider elects to object such requests directly with such authorities.

5.

THIS ADDENDUM IS SUBJECT TO CHANGE UPON THIRTY (30) DAYS PRIOR WRITTEN NOTIFICATION BY PROVIDER TO CLIENT.

The remainder of this page is intentionally left blank.