Exhibit A

VENDOR DATA PROTECTION AND PROCESSING ADDENDUM

This Vendor Data Protection and Processing Addendum ***("DPA")*** is entered into as of the Effective Date (as such term is defined in the Agreement) ***("DPA Effective Date").*** This DPA is incorporated into and forms part of the Agreement (as defined below) between Dexcom, Inc., and its affiliates ***("Dexcom")*** and the entity identified in the Agreement as "Affiliate" (referred to herein as ***"Vendor')*** (collectively, the ***"Parties")***. This DPA reflects the parties' obligations with respect to Personal Data Processed as part of the Services (all as defined below).

In the event of a conflict or inconsistency between the terms of this DPA and the Agreement with respect to the subject matter herein, the terms that are deemed more protective of Dexcom Data shall govern. Any data protection agreements that may already exist between the Parties as of the last signature date of this DPA as well as any earlier version of data security terms to which the Parties may have agreed to are superseded and replaced by this DPA in their entirety. All capitalized terms not defined in this DPA will have the meaning given to them in the Agreement or, if not defined in the Agreement, the meaning given to those terms in the Data Protection Laws.

1. DEFINITIONS

1.1 ***"Agreement'*** means all applicable master agreements, contractor services agreements, terms of service, order forms, purchase orders, contracts, or other legal documents that govern Vendor's provision of the Services or relationship of the Parties, including but not limited to the Stelo Affiliate Agreement.

1.2 ***"Controller"*** means the natural or legal person which alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.3 ***"Data Protection Laws"*** means all applicable laws and regulations regarding the Processing of Personal Data, including, where applicable, the California Consumer Privacy Act of 2018 ***("CCPA"),*** US State Consumer Privacy Laws, or other privacy legislation, each as may be amended from time to time.

1.4 ***"Data Subject"*** means an identified or identifiable natural person. For clarity, Data Subject includes any "consumer" as that term is defined by the CCPA.

1.5 ***"Dexcom Data"*** means all Dexcom data processed by Vendor pursuant to the terms of the Agreement and/or while providing the Services, including Personal Data.

1.6 ***"Personal Data"*** means any information relating to, directly or indirectly, a Data Subject or household that is collected, accessed, used, disclosed, or otherwise Processed by Vendor in its provision of Services, and includes information included in the definition of the terms "personal information," "personally identifiable information," "biometric identifier," or other similar terms under any Data Protection Laws.

1.7 ***"Process(ing)"*** means 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, adaptation or alteration, retrieval, consultation, use, modification, storage, disclosure, restriction, erasure or destruction.

1.8 ***"Processor"*** means a natural or legal person which Processes Personal Data on behalf of the

Controller subject to contractual restrictions consistent and in compliance with Applicable Data Protection Law.

1.9 ***"Services"*** means any products or services, including professional services, provided by Vendor pursuant to the Agreement.

1.10 ***"Subprocessor"*** means any party engaged by Vendor (when acting as Processor on behalf of Dexcom) that Processes Personal Data. Subprocessors are considered "service providers" as such term is defined by the CCPA.

2. GENERAL

2.1 Under the Agreement, Dexcom is acting as a Controller and Vendor is acting as a Processor, or Dexcom is acting as Processor and Vendor is acting as a Subprocessor.

2.2 Vendor certifies that it understands all of its restrictions and obligations under applicable Data Protection Laws and this DPA and shall comply with all Data Protection Laws that apply to its Processing of Personal Data under the Agreement, including, where applicable, Data Protection Laws on collection, sharing, and transfer of Personal Data. Vendor will promptly notify and cooperate with Dexcom if it believes that it can no longer comply with the Data Protection Laws or this DPA in connection with the Agreement. Vendor will, in consultation with Dexcom, take reasonable and appropriate steps to address and remediate such potential noncompliance and will not undertake any Processing in breach of the Data Protection Laws.

3. VENDOR OBLIGATIONS

3.1 GENERAL

Vendor shall:

3.1.1. Process Personal Data only as required for the provision of Services or as explicitly permitted by the Agreement or DPA, and shall not use for any commercial purpose or purposes other than the business purpose(s) specified by the Agreement. Vendor expressly agrees that it shall not sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, Dexcom Data, including any Personal Data contained therein, for monetary or other valuable consideration;

3.1.2. Ensure that all Vendor personnel with access to Personal Data are subject to a duty of confidence, have received appropriate training on their privacy and security responsibilities, and only access such data to perform their duties;

3.1.3. Vendor shall not retain, use, or disclose the Personal Data collected pursuant to Agreement or DPA outside of the direct business relationship between Vendor and Dexcom; and

3.1.4. Keep detailed records of its Processing activities pursuant to the Agreement and this DPA, and shall make those records available to Dexcom at Dexcom's request.

3.2 DELETION OF DATA

Vendor shall return all Dexcom Data at any time during the term of the Agreement upon Dexcom's request and provide Dexcom with thirty (30) days to request the return of Dexcom Data ("Return Period") after termination or expiration of the Agreement. Vendor shall promptly, but in no event later than thirty (30) days after the Return Period, delete all Dexcom Data. Upon request by Dexcom, Vendor shall promptly provide a certificate of deletion of all Dexcom Data.

3.3 COOPERATION.

Vendor shall:

3.3.1. When appropriate, promptly notify Dexcom if it receives any requests from a Data Subject regarding rights afforded under Data Protection Laws ("Data Subject Request"). Vendor shall not respond to any such Data Subject request without Dexcom's prior written consent except to confirm that the request relates to Dexcom;

3.3.2. At Dexcom's determination, either provide Dexcom with the ability to fulfill such Data Subject request independently or shall fully cooperate with Dexcom's reasonable requests so that Dexcom can respond to such Data Subject Requests within the timeframe required under applicable Data Protection Laws;

3.3.3. Vendor shall provide Dexcom with the right to take reasonable and appropriate steps to ensure that Vendor is Processing the Personal Information that is collected pursuant to the Agreement and DPA that is consistent with Data Protection Laws at least every 12 months.

3.3.4. If Dexcom discovers that Vendor is not Processing the Personal Information pursuant the Agreement of DPA, Vendor gives Dexcom the right, upon notice, to take reasonable and appropriate steps to stop and remediate Vendor's unauthorized use of Personal Information.

3.3.5. Vendor shall provide full cooperation and assistance to Dexcom to satisfy Dexcom's compliance obligations to respond to inquiries, investigations, consumer requests, or requests made by a supervisory authority (as defined by Data Protection Laws), in relation to the Personal Data Vendor Processes pursuant to the Agreement; and

3.3.6. When allowed by law, Vendor shall promptly notify Dexcom in the case of an investigation by a government official, audit, or inquiry by a data protection authority or any law enforcement agency regarding the Processing of Personal Data, unless prohibited by applicable law.

3.4 SUBPROCESSORS. Vendor shall submit to Dexcom, in accordance with the notice provisions under the Agreement, a list of its proposed Subprocessors for Dexcom's prior written approval. Any changes to the list of approved Subprocessors must be submitted to Dexcom in writing and are subject to Dexcom's prior written approval. Dexcom may grant or withhold such approval in its sole discretion.

3.4.1. If Vendor engages a Subprocessor to carry out Processing activities on behalf of Dexcom, Vendor shall require the Subprocessor to execute a written agreement to adhere to obligations no less restrictive than those imposed on Vendor in this DPA. Vendor acknowledges that it shall remain fully liable to Dexcom for the performance of its Subprocessors' obligations. For the avoidance of doubt, any and all restrictions on the Vendor's ability to subcontract activities under the Agreement continue in full force and effect, and shall not be limited by the terms of this Section 3.4 (including 3.4.1).

4. CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

4.1 In light of the California Consumer Privacy Act of 2018 (as amended from time to time, the "CCPA") and to ensure that adequate contractual terms are in place between the Parties to comply with the CCPA, the Parties acknowledge and agree that Vendor is a service provider processing Personal Information on behalf of Dexcom.

4.2 For purposes of this Section 5: "commercial purpose," "personal information," "sell," and "service provider" have the meanings given to them in the CCPA; and "Personal Information," with respect to the information of California consumers, has the meaning given in the CCPA to "personal information,"

4.3 Vendor is prohibited from: (i) selling Personal Information and (ii) retaining, using, or disclosing Personal Information for any purpose other than for the specific purpose of performing the agreed upon services, which, for the avoidance of doubt, also prohibits Vendor from retaining, using, or disclosing Personal Information outside of its direct business relationship with Dexcom or for any other

commercial purpose.

5. SECURITY

Vendor shall have in place appropriate technical and organizational security measures to safeguard Dexcom Data, including Personal Data, for protection of the security, confidentiality and integrity of such data, as further described in the Data Security Exhibit attached hereto as Appendix 1 and incorporated herein by this reference.

6. BREACH OBLIGATIONS

6.1 NOTIFICATION REQUIREMENTS. Vendor shall notify Dexcom of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Dexcom Data, including Personal Data contained therein, ***("Breach")*** within seventy-two (72) hours of becoming aware of such Breach. Breach will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

6.1.1. Vendor's notification must:

(i) describe the nature of the Breach including the categories and approximate number of Data Subjects and categories of Personal Data concerned;

(ii) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(iii) describe the likely consequences of the Breach;

(iv) describe the measures taken or proposed to be taken by Vendor to address the Breach, including, where appropriate, measures to mitigate its possible adverse effects; and

(v) include relevant logs, alerts, indicators of compromise, intelligence, and other relevant content that is material to the investigation of the Breach.

6.2 Vendor shall not notify any parties other than Dexcom and, to the extent required by the Data Protections Laws, relevant law enforcement agencies of any Breach without the prior written consent of Dexcom.

6.3 COOPERATION. In the investigation and remediation of any Breach, Vendor shall cooperate with Dexcom's reasonable requests, including providing any necessary information to assist in Dexcom's investigation and in preventing, eradicating, mitigating, rectifying, and responding to such Breach. Vendor agrees that Dexcom may conduct a risk assessment at any time where it becomes aware of a Breach. In the event Dexcom suspects or discovers a Breach in its use of Vendor's Services, Dexcom shall contact Vendor. Vendor shall notify Dexcom of any changes to the contact information during the term of the Agreement.

6.4 COSTS. In addition to any other amounts owed, Vendor shall be liable for all and any damages or losses suffered by or claims against Dexcom relating to a Breach resulting from Vendors' or its Subprocessors' acts or omissions.

7. MISCELLANEOUS

7.1 Upon Dexcom's request, Vendor agrees to enter into additional terms as may be required by Data Protection Law.

7.2 This DPA constitutes the complete and exclusive understanding and agreement of the Parties with respect to the subject matter herein. Any waiver, modification or amendment of any provisions of this DPA will be effective only if in writing and signed by the Parties hereto.

7.3 INDEMNIFICATION. Notwithstanding any provisions elsewhere in the Agreement to the contrary, Vendor shall indemnify Dexcom for any claims, direct or indirect costs, losses, damages, expenses (including legal expenses), and other outgoings sustained by or incurred by Dexcom as a result of or arising out of Vendor's negligence or breach of this DPA.

7.4 LIMITATION OF LIABILITY. NOTWITHSTANDING ANY PROVISIONS OF THE AGREEMENT TO THE CONTRARY, INCLUDING BUT NOT LIMITED TO ANY LIMITATION OF LIABILITY SET FORTH IN THE AGREEMENT, ANY LIMITATION ON VENDOR'S LIABILITY UNDER THE AGREEMENT SHALL NOT APPLY TO A BREACH OR A BREACH OF THE TERMS OF THIS DPA.

7.5 If and to the extent that any provision of this DPA is held to be illegal, void, or unenforceable in any jurisdiction, such provision shall be given no effect in that jurisdiction, but without invalidating any of the remaining provisions of this DPA.

APPENDIX 1: DATA SECURITY EXHIBIT

This Data Security Exhibit describes the minimum technical, organizational, and physical security measures Vendor takes to protect Dexcom Data. Capitalized terms not otherwise defined in this Data Security Exhibit will have the meaning given to them in other parts of the DPA.

1. SECURITY PROGRAM

While providing Services, Vendor will maintain a written information security program of policies, procedures and controls governing the Processing, transmission, and security of Dexcom Data (the ***"Security Program")*** to protect Dexcom Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

Vendor shall regularly test, assess, and evaluate the effectiveness of the Security Program and at least annually review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing threats to the security, confidentiality, and integrity of Dexcom Data, and to ensure that these risks are addressed. For clarity, no such update shall materially reduce the commitments, protections, or overall level of service provided to Dexcom as described herein.

2. PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SECURITY MEASURES

2.1 PHYSICAL SECURITY MEASURES.

2.1.1. Data Center Facilities. (i) Physical access restrictions and monitoring that may include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (ii) fire detection and fire suppression systems both localized and throughout the data center floor.

2.1.2. Systems, Machines, and Devices. (i) Physical protection mechanisms; and (ii) entry controls to limit physical access.

2.1.3. Media. (i) Industry standard destruction of Dexcom Data before disposition of media; (ii) secure safe for storing damaged hard disks prior to physical destruction; and (iii) physical destruction of all decommissioned hard disks storing Dexcom Data.

2.2 TECHNICAL SECURITY MEASURES.

2.2.1. Access Administration. Access to Dexcom Data by Vendor's employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to Dexcom Data. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationships. Production infrastructure includes appropriate user account and password controls (e.g., the required use of VPN connections, complex passwords with expiration dates, and a two-factored authenticated connection) and is accessible for administration.

2.2.2. Access Control. User and role-based access controls.

2.2.3. Logging and Monitoring. Vendor logs activities, which are centrally collected and secured to prevent tampering and are monitored for anomalies by a trained security team. Upon request, Vendor shall promptly make such logs available to Dexcom.

2.2.4. Firewall System. An industry-standard firewall is installed and managed to protect Dexcom Data by residing on the network to inspect all ingress connections routed to the environment.

2.2.5. Vulnerability Management. Vendor conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential

vulnerabilities, and remediate any identified vulnerabilities in a timely manner. When software vulnerabilities are revealed and addressed by a vendor patch, Vendor will obtain the patch from the applicable vendor and apply it promptly and only after such patch is tested and determined to be safe for installation in all production systems.

2.2.6. Antivirus. Vendor updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

2.2.7. Change Control. Vendor ensures that only authorized changes are made to the platform, applications, and production infrastructure. The risk to Dexcom Data shall be assessed and the results of the assessment documented.

2.2.8. Data Separation. Dexcom Data shall be maintained in a separate environment from Vendor's other customers and Vendor's corporate infrastructure.

2.2.9. Encryption. Dexcom data shall be encrypted in transit and at rest in line with industry best practice guidelines.

2.3 ADMINISTRATIVE SECURITY MEASURES.

2.3.1. Data Center Inspections. Vendor must perform routine reviews at each data center to ensure that it continues to maintain the security controls necessary to comply with the Security Program. Where Vendor uses a third-party data center provider, Vendor must perform, at least an annual assessment, to include, where possible an onsite review of the security controls at each data center to ensure continued compliance to the agreements in place, including the DPA and this Data Security Exhibit.

2.3.2. Personnel Security. Vendor performs background screening on all employees and all contractors who have access to Dexcom Data, subject to applicable law.

2.3.3. Security Awareness and Training. Vendor maintains a privacy and security awareness program that includes appropriate training of Vendor personnel on data privacy and the Security Program. Training is conducted at time of hire and at least once per year.

2.3.4. Vendor Risk Management. Vendor maintains a vendor risk management program that assesses all vendors that access, store, process or transmit Dexcom Data for appropriate security controls and business disciplines.

3. SERVICE CONTINUITY AND DISASTER RECOVERY

3.1 Vendor shall implement and document appropriate and adequate business continuity and disaster recovery plans to ensure that Vendor can continue to or resume providing the Services promptly after a disruptive event. Vendor will regularly test and monitor the effectiveness of its business continuity and disaster recovery plans at least annually or as otherwise requested by Dexcom. Vendor shall provide Dexcom with its written business continuity and disaster recovery plan upon request.

4. CERTIFICATIONS AND AUDITS

4.1 CERTIFICATIONS AND ATTESTATIONS. Vendor shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) (collectively, the **"Standards")** for the information security management system supporting the Services. At least once per calendar year, Vendor shall obtain an assessment against such Standards by an independent third-party auditor.

4.2 AUDITS AND CORRECTIVE ACTIONS.

4.2.1. Audits. Vendor shall make available to Dexcom all information necessary to demonstrate

compliance with its obligations under the Agreement and this Data Security Exhibit and allow for and contribute to audits, including remote inspections, conducted by Dexcom or another auditor mandated by Dexcom.

4.2.2. Corrective Actions. Upon request by Dexcom, Vendor shall discuss the results of the audit conducted pursuant to this Section.