DATA SECURITY AGREEMENT (April 2020)

PARTIES	
□ **Aptum Managed Services (Canada) Inc.** whose office is at 191 the West Mall, 2nd Flr., Toronto, M9C 5K8 □ **Aptum Technologies (USA) Inc.** whose office is at Suite 1600, 101 Marietta Street, Atlanta, GA 30303 □ **Aptum Technologies (UK) Limited** whose registered office is at Brettenham House, 2-19 Lancaster Place, London WC2E * (based on entity receiving services under Service Agreement) ("Aptum")	Name: _____ *(include incorporated status)* Address:_____ _____ _____ Details:_____ _____ Address/details for notices (if different to above):_____ _____ ("Company")
Signed for and on behalf of Aptum	**Signed for and on behalf of Company**
Name: Date:	Name: Date:

Governing Law *(Aptum to complete based on legal entity entering into agreement)*

□ *UK*	□ *US*	□ *Canada*
This Agreement shall be interpreted, governed and construed in all respects by the laws of England and Wales.	This Agreement shall be interpreted, governed and construed in all respects by the laws of the state of New York.	This Agreement shall be interpreted, governed and construed in all respects by the laws of the Province of Ontario.

DETAILS OF PROCESSING OF RELEVANT PERSONAL DATA *(to be completed by Aptum where Personal Data is being processed or Customer Environment is being accessed)*

Subject matter and duration of the processing of Relevant Personal Data

The subject matter and duration of the processing of the Relevant Personal Data are set the Service Agreement, any applicable Scope of Work, and this Addendum.

The nature and purpose of the processing of Relevant Personal Data (Describe briefly the reason for using the Company to deliver the Services e.g. migration services for managed hosting solution)

- [Include description here]

The types of Relevant Personal Data to be processed (If known, describe the Personal Data e.g. HR records; financial transaction data etc. If not known state "To be determined by the applicable scope of work")

- [Include list of data types here]

The categories of Data Subject to whom the Relevant Personal Data relates (If known, describe the categories of Data Subject e.g. Employees data, Patient Data, Records of School Pupils etc. If not known state "To be determined by the applicable scope of work"))

- [Include categories of data subjects here]

The obligations and rights of Aptum

The obligations and rights of Aptum (and its clients) are set out in the Service Agreement, any applicable Scope of Work, and this Addendum.

This **Data Security Agreement** (the "**Agreement**") is made on the date of the last signature of the Parties (Aptum and Company, collectively the '**Parties**') in the table above.

WHEREAS:

A. The parties have entered into an Agreement titled [NAME OF AGREEMENT] and dated [INSERT DATE] (the "**Service Agreement**"), pursuant to which the Company has agreed to [INSERT SERVICE DESCRIPTION] (the "**Services**") to Aptum;

B. In order for the Company to be able to perform the Services, it is necessary that the Company have access to systems, networks or facilities owned or managed by Aptum (the "**Information Systems**"). As a consequence of being granted access to the Information Systems, the Company will have access to data created or used in support of Aptum's business activities, which may also include (i) personal information that Aptum has collected from its customers and/or employees or other highly confidential sensitive or critical information (collectively, "**Aptum Information**") or (ii) personal information that Aptum's clients' have collected and are responsible for or other highly confidential sensitive or critical information (collectively, "**Client Information**"). Client Information and Aptum Information together shall be referred to as the "**Restricted Data**". Restricted Data shall include, but is not limited to, documents, reports, plans, designs, processes, know-how, lists, accounts, computer data, business, technical and other information of Aptum or its clients, communicated or made available to the Company, in writing, orally, through visual observation or in any other tangible or intangible form, whether or not marked "confidential", and all notes, analysis, compilations, studies, summaries and other material prepared by the Company containing or based on, in whole or in part, Restricted Data;

C. The purpose of this Agreement is to ensure that any access by the Company to the Restricted Data is made strictly in accordance with the provisions hereto and in compliance with all laws dealing with the protection of the privacy of personal information.

Definitions

1. The following terms shall have the meanings set out below:

Applicable Law: the laws of the jurisdiction stated to be applicable to this Agreement above and any other laws or regulations, regulatory policies, guidelines or industry codes (whether national or international) which apply to Aptum, the Company (or any of its Sub-contractors) and/or the provision of or the subject matter of the Services in each case as in force from time to time.

Data Protection Law: privacy legislation under national, regional or other Applicable Law that applies to the Restricted Data including (but not limited to) in the case of personal data on EU data subjects, (EU) 2016/679 (The General Data Protection Regulation) and any implementing legislation in force from time to time; in the case of personal data on UK data subjects, the Data Protection Act 2018; in the case of personal data on Canadian data subjects, the Personal Information Protection and Electronic Documents Act (PIPEDA); and in respect of US citizens such federal or state legislature as is applicable and relevant to the Services from time to time.

'Data Subject', 'Personal Data', 'Processor' and **'Processing'** shall have the meaning given to them under relevant Data Protection Law.

Responsibilities related to Restricted Data

2. The Parties are each responsible for handling the Restricted Data, and complying with any obligations applying to them, in accordance with Applicable Law and applicable Data Protection Law. The table above sets out certain detail on the Processing of Personal Data as required by Data Protection Law. Aptum may make reasonable amendments to the information stated above by written notice to Company from time to time in order to comply with those requirements.

3. The Company will handle the Restricted Data in accordance with this Agreement and will not use the Restricted Data for any purposes other than those strictly related to the performance of the Services or pursuant to the written instructions of Aptum. The Company agrees that any breach by the Company of its obligations under this Agreement shall also constitute a breach by the Company of the Service Agreement.

4. The Company acknowledges that, to the extent the Restricted Data contains Personal Information, it is a Processor or Sub-Processor, as those terms are defined, under relevant Data Protection Laws. Accordingly, in respect of any Personal Data contained in the Restricted Data, the Company shall:

   4.1 provide any assistance reasonably required by Aptum in order to help Aptum fulfil its obligations under Data Protection Law;

   4.2 process the Restricted Data only on behalf of Aptum for the purposes of performing the Services and only in accordance with instructions contained in this Addendum or otherwise received from Aptum in writing from time to time;

   4.3 not transfer any Restricted Data across national borders unless authorised in writing by Aptum and then subject to any conditions that may be imposed by Aptum; and

   4.4 inform Aptum immediately if, in the Company's reasonable opinion, any instruction from Aptum is in breach of, or is likely to breach, Data Protection Law.

5. Where the Company is obliged by Applicable Law to Process the Restricted Data otherwise than in accordance with clause 4, the Company shall where permitted inform Aptum of that obligation before Processing the Restricted Data giving as much advance notice as is reasonably possible together with a description of the nature and timing of the Processing.

6. The company will not disclose, share or remit the Restricted Data to any third party without the prior written consent of Aptum. For clarity, any agent, consultant, contractor, sub-contractor, provider, affiliate of the Company, shall be considered as a "third party" and this term shall be interpreted as broad as a manner to ensure that disclosure of the Restricted Data remains under control of the Company, at all relevant times.

7. The Company undertakes to inform all employees, consultants and third parties of the confidential nature of the Restricted Data and obtain from such employees, consultant and third parties their commitment to treat the Restricted Data confidentially in the same way as the Company is bound to do so. Any failure by any of the Company's employees, consultants and third parties to so treat the Restricted Data shall be considered as if it were a failure by the Company itself to so treat the Restricted Data and the Company will be responsible for such failure as a breach of this Agreement.

Access Management

8. The Company will only access Restricted Data necessary to perform the Services and shall only disclose and/or provide access to the Restricted Data to those of its employees who have a strict "need-to-know" in order to perform the Services (and to the extent possible, will disclose only that part of the Restricted Data that is necessary for its employees to perform the Services).

9. The Company shall prepare and keep accurate a list of all employees and third parties who may have access to the Restricted Data and, upon request by Aptum, always be able to accurately disclose the list to Aptum.

10. In the event that Aptum owned equipment is loaned to the Company for use at the Company's premises, the Company agrees that such equipment shall only be used in connection with the performance of the Services. Any misuse of or tampering with such equipment and/or its related software shall, in Aptum's sole discretion, be deemed a breach of this Agreement.

Security Requirements

11. The Company shall only connect to the Information System(s) through Aptum's approved method of connections and in accordance with Aptum's security policies and procedures.

12. Where Restricted Information is to be transferred out of a relevant Information System (in agreement with Aptum) to the Company this will be transferred by Aptum via either (i) secure email or (ii) some other agreed secure mechanism of information transfer.

13. Notwithstanding clause 14 below, the Company will take appropriate technical and organisational measures to secure the Restricted Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure and, at Aptum's request, promptly provide a written description of such technical and organisational measures employed by the Company. The Company shall regularly test, evaluate and if necessary improve the security measures to ensure they remain effective and appropriate.

14. The Company agrees that it shall put in place and maintain the security measures outlined in Schedule "A" to this Agreement. Aptum may reasonably add or change any provision of the Information and Cyber-Security Policy at any time, in its sole discretion, upon written notice to the Company. If the requested addition or change materially alters the provision of the Services by the Company, then such change will be managed through a change control process in relation to the Services.

Breach Notification and Access Requests

15. The Company shall immediately (and in any event within 24 hours) notify and advise Aptum:

    15.1 of any known or suspected inappropriate disclosure or use of the Restricted Data or any breach or potential breach of Data Protection Laws; or

    15.2 if it receives any complaint, request for access to Restricted Data or any other communications relating directly or indirectly to the processing of any Restricted Data by the Company,

    and shall co-operate fully with Aptum in any investigation or response related thereto. The Company shall allow Aptum to have access to any records, files, data or information necessary, in Aptum's opinion, for such investigation.

16. Where the Company receives a complaint, request for access or other communication relating to the processing of Restricted Data as referred to in clause 15.2, it shall:

    16.1 respond to that request only on the documented instructions of Aptum or as required by Applicable Laws, in which case Company shall, to the extent permitted by Applicable Laws, inform Aptum of that legal requirement before responding to the request; and

    16.2 provide the Customer with full co-operation and assistance in relation to any complaint, request or other communication made in respect of any Relevant Personal Data, including by (i) providing the Customer with full details of the complaint or request; (ii) complying with the Customer's instructions if a breach of Data Protection Law occurs or is suspected to have occurred; (iii) assisting the Customer in fulfilling the Customer's obligations to respond and comply with requests for exercising the Data Subject's rights pursuant to the Data Protection Law; (iv) providing the Customer with any Relevant

Personal Data it holds in relation to a Data Subject within the timescales required by the Customer; and (v) providing the Customer with any other information relating to the Relevant Personal Data, as may be requested by the Customer.

Audit and Data Impact Assessment

17. Upon reasonable notice, Aptum and its external advisers shall have the right (subject to reasonable and appropriate confidentiality undertakings) to examine any data Processing activities and the measures taken by the Company to safeguard the Information Systems and/or the Restricted Data. The Company shall co-operate fully with Aptum with respect to such examinations to enable Aptum to verify Company's compliance with this Agreement and its obligations under Data Protection Laws. If the Company engages independent third parties to conduct ISO 27001, SOC 2 or other similar audits of the Company, it shall provide a copy of such audit reports to Aptum

18. Company shall assist and cooperate with Aptum in conducting and the implementing any data protection impact assessments Aptum deems necessary.

19. The Company shall maintain complete and accurate records of all information necessary to demonstrate compliance with this Agreement (such records to include but are not limited to: records of staff training; technical and organisational measures taken to ensure compliance with Data Protection Law; and records of processing activities) and make such records available to Aptum or its auditors on request.

Sub-contracting

20. The Company shall not engage any sub-contractor (or allow any existing sub-contractor) to Process the Restricted Data, without obtaining Aptum's prior written consent, and then subject to any conditions that may be imposed by Aptum.

21. With respect to any sub-contractor, the Company shall:

21.1 carry out adequate due diligence in advance to ensure that the sub-contractor is capable of providing the level of protection for Restricted Data required by this Agreement; and

21.2 ensure that it enters into a written agreement with the sub-contractor (i) that includes terms which offer at least the same level of protection for the Restricted Data as set out in this Agreement; (ii) that obliges the sub-contractor to Process any Personal Data contained in the Restricted Data as though it were a party to this Agreement; (iii) meets the requirements of Data Protection Law, and (vi) to provide a copy of the same as Aptum may request from time to time (which may be redacted of commercial information not relevant to the requirements of this Agreement).

21.3 The Company shall remain fully liable to Aptum for the performance of any sub-contractor's obligations and shall be fully liable for the acts or omissions of the sub-contractor.

Effect of Termination and Data Retention

22. Upon the expiry or termination of the Service Agreement, or at any time upon the request of Aptum, the Company will disconnect all connections made by it to the Information Systems and will return to Aptum any Restricted Data or certify that it has destroyed the Restricted Data in a manner designated by Aptum or otherwise agreed to by the parties. Where the Company is obliged by Applicable Law to retain certain Restricted Data, it shall comply with its obligations under this clause 22 as soon as is permissible under Applicable Law.

Indemnity

23. The Company agrees to indemnify and hold harmless Aptum and its directors, officers, employees and agents from any and all losses, damages, costs or expenses (including reasonable legal fees

and disbursements) suffered or incurred by Aptum attributable to any failure of the Company to perform its obligations under this Agreement.

General

24. Notices or other document or correspondence required or permitted to be given under this Agreement shall be in writing and shall be deemed to have been properly given one (1) day after dispatch by registered or certified mail, one (1) day after dispatch by facsimile transmission, addressed to the party to whom it was sent at the address, or facsimile number, of such party set forth on the first page above or at such other address or facsimile as the party shall subsequently designate to the other party by notice given in accordance with this clause or on the date of actual delivery if delivered by hand or by courier.

25. No amendment to this Agreement shall be binding on the parties unless made in writing and signed by an authorized representative of each of the parties.

26. This Agreement shall enure to the benefit of and shall be binding upon the parties and their respective successors and assigns.

[Appendix A follows]

Appendix A: Aptum Security Requirements

	A. General security requirements
A.1	Ensure that the organization has defined support for information security and has a security program in place to support its business needs.
	B. Information security policies
B.1	Define an Information Security Policy approved by management and communicated to all employees and relevant external parties. The policy must be reviewed annually. If no policy exists, or if the Company has access to Aptum's or Aptum's clients Information Systems, Company is required to comply with Aptum's Information Security Policy (attached below).
	C. Organization of Information Security
C.1	Define and assign Information Security responsibilities including the Chief Information Security Officer role (or equivalent).
C.2	Supplier shall ensure information security roles and responsibilities are documented.
	D. Human resource security
D.1	Ensure that for all employees and contractors, a confidentiality clause is included either in the employment contract or in the relevant agreement.
D.2	Enforce and communicate Information security policy and a continuous Security Awareness Program for each employee and contractor.
D.3	Have documented controls to disable Supplier's employees, contractors and temporary staff access to any asset or system used to provide services to Aptum or access its Information Systems immediately after departure or when no longer required.
	E. Asset management
E.1	Develop and maintain a register of assets used to deliver the Services and/or Process the Restricted Data to Aptum.
E.2	Securely erase the Restricted Data in Company's possession, using industry best practices, when no longer required.
	F. Access control
F.1	Adopt organizational measures to permit access to the Restricted Data only by duly authorized persons.
F.2	Enforce a formal procedure to manage any privileged accounts used by the Company employees and contractors to provide the Services.
F.3	Enforce the use of personal (individual user) accounts in order to be able to identify each action to a specific user. If not possible, a formal process must exist in order to be able to identify the owner of each action (e.g. logs).
	G. Cryptography
G.1	Ensure that all Restricted Data transfered from a relevant Information System is encrypted both in transit and at rest.
G.2	Ensure the implementation of a process to protect and manage the lifecycle of cryptographic keys and passwords.
	H. Physical and environmental security
H.1	Implement physical access controls on premises where the Restricted Data is stored / processed in such a manner that physical access is only permitted for authorized persons or persons accompanied by authorized personnel.
H.2	Use data center(s) that have appropriate physical and environmental controls that are audited by an independent third party auditor. Appropriate physical and environmental controls may be determined via an industry certification such as SOC 2, PCI DSS and/or ISO 27001 as may be appropriate in respect of the Services being delivered.
	I. Operations security

I.1	Define and apply, on all security devices, network components, servers and middleware used to provide the Services - configuration standards and operational guides that follow best practices such as those from National Institute of Standards and Technology (NIST) or Centre for Information Security (CIS).
I.2	Ensure adequate change management processes are in place within the Company to ensure changes to Company systems are reviewed, approved and will not impact the Services provided by the Company
I.3	Take any necessary precautions to prevent Malware infection of the systems used to provide the Services and the introduction of any Malware in Aptum's Information System.
I.4	Implement all necessary measures in terms of backup and restore to comply with the agreed upon Recovery Point Objective (defined, including regular tests of the reliability and completeness of the backups.)
I.5	Logging - Keep and ensure integrity of audit logs with a retention period of at least 12 months. At minimum logs must contain remote IP addresses and timestamp for the following events: a) Failed & Successful logon. b) All Privileged Accounts actions.
	c) Password reset by users. d) Refused access to Data (i.e. permission denied)
I.6	Monitor Security Advisories from vendors of all hardware and software used to provide the Services, on a periodic basis. Remediate any identified vulnerabilities in no delay.
I.7	Install applicable security hotfixes (or workaround) recommended by hardware / software vendors within an acceptable period. Aptum reserves the right to information on the Company's patching policy.
	J. Communications security
J.1	Restrict - at network-level - any access from Internet to private infrastructures services, operating systems and middleware interfaces (e.g. Database listener, SSH, back-end API...) used to provide the Services.
J.2	Ensure any remote Privileged Account access from Internet to the Supplier's infrastructure enforce strong encryption and Multi-Factor Authentication.
J.3	Apply Company XYZ remote access procedures to access Company XYZ Information System for the purpose of the Services, including: - Protect all credentials provided by Company XYZ. - Use remote access only when required by Company XYZ to perform the Services. - Keep logs of who used the credentials with a retention period of 12 months.
	K. System acquisition, development and maintenance
K.1	Guarantee that Restricted Data is never exported to or used in a non-production environment (including for testing purposes) without previous formal approval of Aptum.
	L. Supplier relationships
L1	Company must have vendor management processes in place to manage its sub-contractors in accordance with the obligations under this Agreement.
L.2	Monitor and review on a regular basis compliance by its sub-contractors used to provide these security obligations.
	M. Incident management
M.1	Define an Information Security Incident management procedure (including illegitimate access to Aptum's systems and/or Restricted Data used to deliver the Services) and implement an incident mitigation plan and identify root cause analysis if such incidents occur.
M.2	Maintain an updated procedure specifying when and who to call at Aptum in case of a Security Incident.
	N. Business continuity

N.1	Adopt technical and organizational business continuity measures to ensure Services are provided according to service level objectives.
N.2	Ensure that the Disaster Recovery Plan (DRP) and any response plans are tested and updated annually in order to ensure that they are valid and effective during adverse situations.
	O. Compliance
O.1	Maintain throughout the term of the Agreement, at its own costs, audits and/or certification(s) agreed with Aptum within the Agreement duration, and communicate immediately, upon Aptum's request, all documentation regarding such audit and/or certifications.
O.2	When the Supplier is directly involved in the processing, storage, or transmission of cardholder data, on behalf of Aptum, comply with PCI-DSS standard (https://www.pcisecuritystandards.org/) and provide Aptum with the related proof of certification (Attestation of Compliance) on a yearly basis.

[Attached: Aptum – Information Security Policy]

(See PDF)