Effective February 03, 2026. This Canadian Data Privacy Agreement supersedes and replaces all prior versions.

Canadian Data Processing Agreement

This Canadian Data Processing Agreement (the "DPA") between Provider (sometimes referred to as "Provider," "we," "us," or "our"), and the Client found on the applicable Order (sometimes referred to as "you," or "your,") and, together with the Order, Master Services Agreement ("MSA"), Schedule of Services and other relevant Service Attachments identified in Exhibit A to the Order, forms the Agreement between the parties the terms to which the parties agree to be bound.

PIPEDA - This DPA reflects the requirements of the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA") of 2004 and its implementing regulations, as amended or superseded from time to time (S.C. 2000, c. 5).

This Agreement shall only apply and bind the Parties if and to the extent of the activity between the Parties is considered "Commercial Activity" under PIPEDA. This DPA prevails over any conflicting terms of the MSA, but does not otherwise modify the MSA. All capitalized terms not defined in this DPA shall have the meanings set forth in the PIPEDA. Client enters into this DPA on behalf of itself and, to the extent required under the PIPEDA, in the name and on behalf of Client's Authorized Affiliates (defined below).

In the course of providing Services to Client pursuant to the Agreement, Provider may be requested or required to process Personal Information provided by or collected on behalf of Client. This DPA sets out additional terms, requirements, and conditions for collecting, using, disclosing, transferring, storing, or otherwise processing Personal Information when Provider provides Services under the Agreement.

DEFINITIONS

"Affiliate" means an entity that directly or indirectly controls, is controlled by or is under common control with an entity.

"Authorized Affiliate" means any of Client's Affiliate(s) permitted to or otherwise receiving the benefit of the Services pursuant to this DPA.

"Applicable Law" means all present and future laws, statutes, ordinances, regulations, judgements, orders, rules, and directions of any court or governmental authority that are enforceable in Canada, and includes Applicable Privacy Law;

"Applicable Privacy Law" means any and all privacy and data protection and processing laws, statutes, regulations, judgements, orders, rules and directions of any court or governmental authority that may be applicable in the circumstances, which may include, without limitation, the Personal Information Protection and Electronic Documents Act (Canada) and regulations thereunder ("PIPEDA"), provincial privacy legislation deemed substantially similar to PIPEDA and/or provincial personal health information legislation;

"Commissioner" means the applicable federal or provincial privacy commissioner having jurisdiction over privacy and data protection matters;

"Conflicting Foreign Order" means any order, subpoena, directive, ruling, judgment, injunction, award or decree, decision, request or other requirement issued from a foreign court, agency of a

foreign state or other authority outside Canada or any foreign legislation the compliance with which would or could potentially breach Applicable Privacy Law;

“Confidentiality Agreement” means a standard agreement between Provider and its Personnel, signed as part of Provider’s operating procedures, requiring that Personnel comply with the requirements of Applicable Privacy Law, and other Applicable Law, in a manner which is intended to ensure compliance by Provider and its Personnel under this DPA;

“Contact Information” means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address and business email of the individual;

“Excluded Information” or “Excluded Records” means information, documents or recorded information that (a) relate solely to Provider’s internal administration, finances, management, or labor and employment matters, unless they contain Personal Information about an individual other than Personnel or other third parties with whom Provider has dealings unrelated to the subject matter of the DPA; or (b) Client confirms in writing are excluded from the application of this DPA;

“Material Breach” means non-compliance or contravention by Provider with any provision of this DPA or Applicable Privacy Law relating to or resulting from the collection, use, disclosure, storage, disposal or destruction, or other processing by Provider of any Personal Information or Records;

“Permitted Purpose” means access to, use, or processing of the Records or Personal Information that is necessary for provision of the Services;

“Personal Health Information” means personal health information about an individual as defined by Applicable Privacy Law;

“Personal Information” means information about an identifiable individual within the meaning of Applicable Privacy Law, excluding Contact Information (to the extent excluded by Applicable Privacy Law) and Excluded Information, that is collected or created by Provider or otherwise obtained or held by or accessible to or processed by Provider as a result of the DPA, and specifically includes Personal Health Information;

“Personnel” means any employees, officers, directors, contractors, subcontractors, associates, representatives or other persons engaged by Provider for the purposes of fulfilling Provider’s obligations under the DPA;

“Privacy Representative” means, as applicable, the designate of Provider or Client with responsibility for such party’s compliance with Applicable Privacy Law and this DPA; and

“Processing”, “processes” or “process” means any activity that involves the use of Personal Information, including, without limitation, obtaining, collecting, recording, or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it, and transferring it to third parties.

“Record” includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which Personal Information is recorded or stored by graphic, electronic, mechanical or other means which are collected or produced by Provider in the course of delivering Services or otherwise performing its obligations under the DPA, but does not include Excluded Records.

PROVIDER SUBJECT TO APPLICABLE LAW

© Scott & Scott,

Provider agrees that, in relation to the collection, use, processing, sharing, disclosure, storage, security, destruction and management or administration of Personal Information and Records, it is subject to and will comply with the requirements of Applicable Privacy Law and this DPA, including any applicable order or security requirements prescribed by the Commissioner or a court. Provider will ensure that it and its Personnel are familiar with its and their obligations under Applicable Privacy Law and this DPA.

Provider acknowledges that Personal Information may be disclosed to Provider for the sole purpose of performing the Services. Provider shall exercise all reasonable precautions to protect Personal Information from unauthorized access, disclosure, copying, use, modification, storage or retention and, in any event, treat any information which is Personal Information in accordance with Applicable Privacy Law and this DPA. In particular, the use of Personal Information must be restricted to the Permitted Purpose in compliance with Applicable Privacy Law, unless otherwise authorized by Client in writing or required or authorized by Applicable Law.

Provider agrees that if it is a “service provider”, “information manager”, “information management service provider” or “agent” as defined in Applicable Privacy Law, as a result of the type of Services that it is providing to Client under the DPA, Provider shall comply with its obligations under Applicable Privacy Law in that regard.

Provider agrees to maintain a privacy policy in compliance with Applicable Privacy Law.

Provider specifically assumes all responsibility for its Personnel and for the breach by any one or more of them of any provision of Applicable Privacy Law or this DPA.

CONTROL OF AND RIGHTS IN THE RECORD(S) AND CONSENT

The Parties acknowledge and agree that as between Client and Provider:

- All right, title, interest and control in and to all Records and Personal Information shall remain with Client. No proprietary right or other interest respecting the Records or Personal Information, other than as expressly set out in this DPA and the Agreement, is granted to Provider under this DPA or the DPA, by implication or otherwise. Provider is granted temporary access to the Personal Information on the terms and conditions of this DPA, for the sole and express purpose of performing the Services and for no other use or purpose except as authorized by Client in writing or required or authorized by Applicable Law. Where Provider provides services under contract with one or more other parties in which such other parties also assert control over the same or overlapping Records, Client will work with such other parties to resolve each other’s rights and obligations with respect to such Records and Provider will not be considered to be in breach of this DPA by reason of its inability to provide unfettered control over the Records to Client.
- It is the responsibility of Client to identify and have directly or indirectly obtained any consent from, and/or given any notice to, individuals as required under Applicable Privacy Laws, for Provider’s collection, use, processing, sharing, disclosure, storage, security, destruction, management or administration of Personal Information under the Agreement. If Client requires Provider to collect Personal Information on its behalf in the course of providing Services, Client will identify to Provider any requirements of Applicable Privacy Law regarding collection of the Personal Information.

© Scott & Scott,

COLLECTION, USE & DISCLOSURE OF PERSONAL INFORMATION

Provider will only collect, use, disclose, and otherwise process Personal Information on behalf of Client as necessary for the performance of the Services or as otherwise authorized by Client in writing or required or authorized by Applicable Law.

Provider will ensure that neither it nor its Personnel collects, creates, copies, reproduces, uses, stores, discloses, provides access to, or otherwise processes any Personal Information except in compliance with this DPA and Applicable Privacy Law and for purposes directly related to or necessary for the performance of the Services or as otherwise authorized by Client in writing or required or authorized by Applicable Law.

REFERRAL OF REQUESTS FOR ACCESS OR CORRECTION

If Provider receives a request under Applicable Privacy Law for access to or correction of Personal Information from a person other than Client, Provider will promptly advise the person to make the request to Client and provide the name and contact information for Client's Privacy Representative, and Provider shall notify Client of any such request.

COOPERATION IN RESPONDING TO REQUESTS FOR ACCESS

Where Client communicates to Provider that it has received a request for access to Personal Information, Provider will locate and supply to Client any and all Records in its custody that fall within the scope of the request. Provider will comply with this obligation within a reasonable period that allows Client to comply with its obligations under Applicable Privacy Law.

ACCURACY AND CORRECTION OF PERSONAL INFORMATION

If Provider engages in the collection, maintenance or updating of Personal Information or the creation of Records on behalf of Client under the DPA, Provider will make every reasonable effort to ensure the accuracy and completeness of such Personal Information generally and as required by Applicable Privacy Law.

PROTECTION & SECURITY OF PERSONAL INFORMATION

Provider shall protect Personal Information in compliance with Applicable Privacy Law, by making reasonable security arrangements appropriate to the sensitivity of the insformation to protect such Personal Information against such risks as theft, loss or unauthorized access, collection, use, disclosure, copying, modification, destruction, or disposal.

ACCESS BY PERSONNEL

Provider will ensure that its Personnel are granted access to the Personal Information only where such access is necessary for the performance of the Services, and subject to the following terms:

- Prior to access, Provider has entered into its standard Confidentiality Agreement with its Personnel or Provider's Personnel has expressly agreed to comply with Provider's internal documents acknowledging the obligations of protecting Personal Information pursuant to this DPA and Applicable Privacy Law;
- Provider will revoke the access rights of any person who engages in the unauthorized access to or collection, use or disclosure of Personal Information or otherwise breaches the Confidentiality Agreement or Applicable Privacy Law; and
- Provider will ensure Personnel with access to Personal Information are familiar and comply with the obligations of Provider under this DPA and Applicable Privacy Law.

© Scott & Scott,

SUBCONTRACTORS

Provider acknowledges that if it uses subcontractors to perform any Services for Client that will require access to or processing of Personal Information, it will require such subcontractors to be bound by terms equivalent to this DPA and Applicable Privacy Law.

ACCESS AND STORAGE OUTSIDE OF CANADA

Client hereby acknowledges and agrees that Personal information and Records may be collected, used, processed, shared, disclosed, stored, secured, destroyed, managed or administered from outside of Canada by Provider using cloud computing of other information technology infrastructure selected by Provider and managed using third parties, and that Client has provided or will provide all required notices and information and/or has obtained or will obtain all required consents and approvals for such collection, use, processing, sharing, disclosure, storage, security, destruction, management and administration outside of Canada, in compliance with Applicable Privacy Law.

NOTICE OF DEMANDS FOR DISCLOSURE

If Provider becomes legally compelled or otherwise receives a demand to disclose Personal Information other than as permitted by Applicable Privacy Law, including without limitation pursuant to any Conflicting Foreign Order, unless prohibited by law, Provider will not do so unless and until: (i) Client has been notified of such requirement; (ii) the parties have appeared before a Canadian Court; and (iii) the Canadian Court has ordered the disclosure. Provider is responsible to ensure that it obtains such contractual rights or makes other such arrangements with its Personnel or such other third parties to whom it may grant access to Personal Information as may be necessary to enable it to comply with the provisions of this Section. Nothing in this DPA will be interpreted or construed to prohibit Provider from complying with any valid court order made under the laws of Canada applicable in the Province.

AGGREGATE AND DE-IDENTIFIED DATA

Notwithstanding the provisions of this DPA, Provider retains the right to use and disclose aggregated and De-Identified Data in any manner permitted by Applicable Law. “De-Identified Data” means information (or any portion thereof) that has been the subject of reasonable efforts to de-identify, aggregate and/or anonymize such data with the result that no individual can be identified, such that it is no longer Personal Information as defined in Applicable Privacy Laws.

PRIVACY REPRESENTATIVE

Each of Provider and Client will appoint a Privacy Representative and such person will have sufficient authority to make decisions and execute documents on behalf of such party as may be required from time to time for the administration of this DPA. Each party shall promptly provide the other party with the name and contact details of its Privacy Representative and shall notify the other party of any change of its Privacy Representative.

NOTICE OF BREACH AND CORRECTIVE ACTION

Provider will provide Client with prompt written notice of any actual or reasonably anticipated Material Breach, including full particulars of such breach.

© Scott & Scott,

Provider will reasonably cooperate with Client in preventing the occurrence or recurrence of any breach of this DPA or Applicable Privacy Law, including, if requested to do so: by preparing a written proposal to address or prevent further occurrences within Provider's systems.

INSPECTION, INVESTIGATION & COOPERATION

Upon reasonable request by Client, Provider will provide information to a Commissioner pertaining to Provider's handling of Personal Information pursuant to this DPA, the Agreement and Applicable Privacy Law, including:

- Provider's privacy policy; and
- information regarding any complaints against Provider to a Commissioner.

Provider will reasonably cooperate at Client's cost with Client in the event of any audit, investigation, inquiry, complaint, suit or other legal proceeding regarding any actual or alleged breach of Applicable Privacy Law or this DPA, for a Material Breach.

RETURN OR DESTRUCTION OF THE RECORD UPON REQUEST

Except as otherwise specified in the Agreement, Provider will retain the Personal Information and Records until it is provided with a written direction from Client regarding its return or destruction.

Upon the expiry or earlier termination of the Agreement or, at any time upon the written request of Client, Provider will promptly: (i) return or deliver all Records, including any copies thereof, to Client; or (ii) destroy, according to Client's instructions, all Records, including any copies thereof, in any form or format whatsoever in Provider's possession constituting or based upon Personal Information.

After a request is made under this Section, Provider will not retain any Records for any purpose without the prior written consent of Client, save and except as required by Applicable Law. If, for any reason, Provider fails to return or destroy any Record in accordance with this Section, Provider's obligations pursuant to this DPA will continue in full force and effect.

GENERAL

The parties acknowledge and agree that either party may disclose the DPA or portions thereof as may be required pursuant to Applicable Privacy Law.

If a provision of this DPA or the Agreement conflicts with a requirement of Applicable Privacy Law, the conflicting provision of the Agreement will be inoperative to the extent of the conflict.

Unless otherwise expressly provided in the Agreement, if a provision of this DPA is inconsistent or conflicts with a provision of the Agreement, the conflicting or inconsistent provision in the Agreement will be inoperative to the extent of the conflict.

Provider's obligations under this DPA will continue despite the expiry or earlier termination of the Agreement until such time as the Personal Information and Records are returned to Client or securely destroyed in accordance with this DPA.

PERSONAL HEALTH INFORMATION PROTECTION ACT, 2004 (ONTARIO) ("PHIPA")

In this section of this DPA,

"health information custodian" has the meaning set out in PHIPA;

"personal health information" has the meaning set out in PHIPA; and

© Scott & Scott,

“PHIPA” means the Personal Health Information Act, 2004 (Ontario) and regulations thereunder.

Uses and Disclosures of Personal Health Information

If the Order references PHIPA, Provider and Client acknowledge that Client is a health information custodian to which PHIPA applies. In provision of Services to Client, including, as applicable, website hosting services and other managed information technology services, Provider may have access to certain personal health information collected by or on behalf of Client or otherwise provided by Client to Provider. Provider will safeguard any such personal health information it receives in accordance with this DPA and Applicable Privacy Law, and will not use that information for any purpose other than as necessary in the provision of Services to Client, and will not disclose that information to any third party except in accordance with this DPA and the Agreement or as required by Applicable Law. In addition, Provider will not permit its Personnel or any person acting on Provider’s behalf to be able to have access to such information unless they agree to comply with the restrictions equivalent ot those that apply to Provider.

Consent

Client must obtain individual consents to Provider’s collection, use, or disclosure of that personal information, in accordance with the PHIPA Privacy Policy and as permitted or required by law. The PHIPA Privacy Policy should also note that an exception to requiring consent may be made in cases of legal, medical, or security reasons where it is impossible or impractical to receive consent.

Patients’ rights regarding marketing information

Receiving marketing communications, whether in hard copy or by email, is always optional, and patients will be provided every opportunity to be removed from email or address lists containing such communications. Patients can unsubscribe from email marketing communications by following the links sent to them by Client. Provider will not send marketing messages to patients.

Personal information is treated as private and confidential

Provider will protect personal health information by providing security safeguards that are appropriate to the sensitivity of the information. Provider will only retain personal health information for as long as it is required to perform Services or as required by Applicable Law. Although Provider makes every reasonable effort to protect personal information from loss, theft, unauthorized access, release, use, disclosure, alteration by third parties, copying, or modification by the use of reasonable security safeguards, including physical and logical security procedures, confidentiality policies, and authorization requirements, there is always some risk involved in transmitting information over the Internet. Because of this, Provider does not represent, warrant or guarantee that personal health information will be protected against theft, loss, unauthorized access, use, disclosure, or alteration, and does not accept any liability for personal health information submitted by patients to Client or to Provider, nor for patients’ or third parties’ use or misuse of personal health information provided by Client or Provider on behalf of Client.

Website.

Individuals may visit the public portion of Provider’s website without providing any personal information. Provider may collect some information regarding patient use on its website and the pages patients visit on the website. This “use” can include the type of browser a patient uses, and the name of the patient’s Internet Service Provider. Provider may collect “cookie” information from patients’ browsers to identify their computers and provide the health information custodian with a

© Scott & Scott,

record of patient visits to the website. Users may set their browser to disable or refuse to accept cookies, although doing so may affect their viewing of certain portions of the website.

HEALTH INFORMATION ACT (HIA) – This DPA is intended to establish the rules governing the collection, storage, and disclosure of health information by the Information Manager and the terms upon which the Physician(s) may access, use or disclose stored health information, all in compliance with s. 66 of the HIA.

The guiding principles in the HIA, include the use and disclosure of the least amount of health information necessary to achieve the purposes.

DEFINITIONS

Unless otherwise specified, capitalized terms in this DPA shall have the meanings ascribed to such terms in the Health Information Act ("HIA")

"Health Information Act" or "HIA" means the Health Information Act, R.S.A. 2000, c. H-5, as amended from time to time and the regulations thereunder;

"Electronic Medical Record" or "EMR" means the collection of health information relating to the Patients of the custodian(s) stored in an electronic format and managed by the Information Manager;

"Information Management Agreement" means this DPA;

"Information Management Services" means the services provided by the Information Manager to the Physician(s) in accordance with the provisions of this Information Management Agreement;

"Patient" means an individual who attends a physician for the purposes of receiving medical care;

"Physician(s)" means a medical doctor licensed to practice medicine in the Province of Alberta, includes physicians practicing through Professional Corporations, physicians practicing as partnerships, or in association with other physicians ("the Physician Group");

"System" means the EMR software utilized by the Physician(s) in the course of performing their clinical responsibilities for Patients;

"Third Parties" means individuals or other entities who are not party to this Information Management Agreement.

CONTINUING CONSENT OF CLIENT

Client consents to the release of health information to Provider in accordance with, and for the purposes outlined in this DPA.

If an Authorized Representative is designated, the Authorized Representative warrants that all Physician(s) who are members of the Physician Group of Client from time to time have provided their consent to the release of health information to Provider on the terms and conditions outlined herein.

APPOINTMENT AND DUTIES OF INFORMATION MANAGER

Client hereby appoints Provider to act as its Information Manager.

Provider may receive and store health information relating to a Patient's clinical treatment within the clinic.

© Scott & Scott,

Provider may use health information in its custody and control for any of the purposes outlined in this Information Management Agreement.

Provider may disclose health information in a non-identified (aggregate) basis, to any custodians who are parties to this Information Management Agreement. Provider may disclose identifiable data to a physician responsible for or involved in the treatment or management of the Patient.

Provider may disclose health information to Third Parties, as authorized by the HIA and in accordance with the specific directions from the Physician(s).

In providing the Information Management Services in accordance with this DPA, Provider will need to have access to, or may need to use, disclose, retain or dispose of the some or all of the health information.

Provider shall not collect health information; only the Physician(s) may collect health information in accordance with s. 20 of the HIA, and use the health information in accordance with s. 27 of the HIA.

Disclosure to Physician(s) or Third Parties shall be for the following purposes:

- For ongoing patient care;
- For medical practice audits;
- For data counts or statistical purposes;
- For research conducted on aggregate health information; or
- For research requiring individualized data.

Provider shall store and disclose health information strictly in accordance with the terms of this DPA and the HIA and any other applicable legislation in force in the Province of Alberta and will not allow access to stored health information to any person other than for the purposes referenced in this DPA.

The Parties agree that all stored health information is private and confidential. Provider will take reasonable steps to maintain that confidentiality, including termination of this Information Management Agreement with Physicians determined to be in breach of this Information Management Agreement.

Client warrants and represents that the health information has been gathered and stored with the consent of the patient who owns the health information contained therein.

CONFIDENTIALITY

Provider shall treat all health information that it has access to under this Information Management Agreement as confidential. Only those employees or agents of the Information Manager who are engaged in information management services shall have access to health information.

Provider shall take all reasonable steps to prevent the unauthorized disclosure of health information.

Provider shall limit its use and disclosure of health information to only the minimum necessary health information required by Provider to furnish services or resolve support issues on behalf of Client.

Should any unauthorized disclosure of health information occur, Provider shall forthwith provide immediate notification to Client, including the particulars of the disclosure. Provider shall take all reasonable steps to mitigate the disclosure immediately and on an ongoing basis, as required.

© Scott & Scott,

Provider may disclose health information to any other information managers used by Client with authorization from the physicians.

PATIENT REQUEST FOR INFORMATION

Any expressed wishes from a Patient relating to health information, including access requests and requests to amend or correct health information under Part 2 of the HIA, will be directed to Client. Provider will not take any other action without authorization by the Physician(s).

Any requests under clause 24 must be forwarded, in writing, to Client within 48 hours of receipt of that request.

Patient requests for information shall, where possible, be responded to by Client within five (5) business days of the receipt of the request.

PROTECTION AND SECURITY OF HEALTH INFORMATION

Provider, its employees, subcontractors and agents shall protect the health information against such risks as unauthorized access, use, disclosure, destruction or alteration.

Provider, its employees, subcontractors and agents must not modify or alter the health information unless it is required as part of the information management services and only on the written instructions of Client.

RETENTION AND DESTRUCTION OF HEALTH INFORMATION

No health information in the custody and control of Provider shall be stored outside of the Province of Alberta.

No health information in the custody and control of Provider shall be destroyed or disposed of without the express written consent of Client.

TERMINATION

Upon termination of this Information Management Agreement, Provider will ensure that the health information is returned to Client who have contributed the health information, together with all modifications, additions and enhancements in a mutually acceptable format, failed following which any remaining copies will be destroyed.

Upon termination, Provider shall not disclose health information contributed by the Physician(s) without the express consent of the Patient who is the subject matter of the health information, unless the disclosure is done in a non-identifiable or aggregate manner.

© Scott & Scott,