Effective February 14, 2024. This Canadian Data Privacy Agreement supersedes and replaces all prior versions.

Canadian Data Processing Agreement

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

PIPEDA - This Canadian Data Privacy Agreement (the "Agreement") 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Information Protection and Electronic Documents Act ("PIPEDA") of 2004 and its implementing regulations, as amended or superseded from time to time (S.C. 2000, c. 5).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 makes clear that Provider is acting as a "Service Provider" for PIPEDA purposes.

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 Agreement prevails over any conflicting terms of the Agreement, but does not otherwise modify the Agreement. All capitalized terms not defined in this Agreement shall have the meanings set forth in the PIPEDA. Client enters into this Agreement 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).

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 Clients' Affiliate(s) permitted to or otherwise receiving the benefit of the Services pursuant to the Scope and Applicability of this Agreement.

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

"Applicable Privacy Law" means any privacy legislation that may be applicable in the circumstances, which may include the Personal Information Protection and Electronic Documents Act ("PIPEDA"), provincial legislation deemed substantially similar to PIPEDA and/or provincial health information legislation;

"Commissioner" means the Information and Privacy Commissioner as applicable;

"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 Agreement;

“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 Agreement; or (b) Client confirms in writing are excluded from the application of this Agreement;

“Material Breach” includes, without limitation, (i) non-compliance by Provider with any provision of this Agreement relating to or resulting from the collection, use, disclosure, storage, disposal or destruction of any Personal Information or Records in contravention of Applicable Privacy Law and/or this Agreement; and (ii) non-compliance by Provider to take reasonable steps to cure any contravention of Applicable Privacy Law and/or this Agreement to the satisfaction of Client within 30 days after written notice is given to Provider describing the breach in reasonable detail or otherwise within 30 days of Provider becoming aware of the breach;

“Permitted Purpose” means access to Records or Personal Information that is necessary for provision of the Services (as defined in the Agreement);

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

“Personal Information” means recorded information about an identifiable individual, excluding Contact Information and Excluded Information, that is collected or created by Provider or otherwise obtained or held by or accessible to Provider as a result of the Agreement or any previous agreement between Client and Provider dealing with the same subject matter as the Agreement, 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 Agreement;

“Privacy Representative” means the designate of Provider or Client with responsibility for compliance with Applicable Privacy Law and this Agreement; and

“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 Agreement, but does not include Excluded Records.

PROVDIER SUBJECT TO APPLICABLE LAW

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 Agreement, 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.

Provider acknowledges that Personal Health Information may be disclosed to Provider for the sole purpose of performing the Services. Provider shall exercise all reasonable precautions to protect Personal Health Information from unauthorized access, disclosure, copying, use or modification, storage and retention and, in any event, treat any information which is Personal Health Information in accordance with Applicable Privacy Law. In particular, the use of Personal Health Information must be restricted to the purposes and activities as outlined in Applicable Privacy 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 Agreement, Provider agrees to 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 the Personnel and for the breach by any one or more of them of any provision of Applicable Privacy Law or this Agreement.

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 shall remain with Client. No proprietary right or other interest respecting the Records, other than as expressly set out herein, is granted to Provider under this Agreement or the Agreement, by implication or otherwise. Provider is granted temporary access to the Personal Information on the terms and conditions of this Agreement, for the sole and express purpose of performing the Services and for no other use or purpose. 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 Agreement 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, 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. If Client requires Provider to collect Personal Information on its behalf pursuant to this Section, Client will identify to Provider any requirements of Applicable Privacy Law regarding collection of the Personal Information.

COLLECTION, USE & DISCLOSURE OF PERSONAL INFORMATION

Provider will only collect, use and disclose 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 or provides access to any Personal Information except in compliance with this Agreement and Applicable Privacy Law and for purposes directly related to or necessary for the performance of the Services or as otherwise required 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 Agreement, 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 must protect Personal Information to ensure compliance with Applicable Privacy Law, by making reasonable security arrangements against such risks as theft, loss or unauthorized access, collection, use, disclosure 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 Agreement and Applicable Privacy Law;
- Provider will revoke the access rights of any person who engages in the unauthorized 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 Agreement and Applicable Privacy Law.

SUBCONTRACTORS

Provider acknowledges that if it uses subcontractors to perform any services for Client that it will require subcontractor to be bound by terms equivalent to this Agreement and Applicable Privacy Law.

ACCESS AND STORAGE OUTSIDE OF CANADA

Client hereby acknowledges and consents 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 all required notices and information and/or obtained all required consents and approvals for such collection, use, processing, sharing, disclosure, storage, security, destruction, management and administration outside of Canada.

NOTICE OF DEMANDS FOR DISCLOSURE

If Provider or anyone to whom Provider transmits Personal Information pursuant to a Permitted Purpose becomes legally compelled or otherwise receives a demand to disclose Personal Information other than 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 Agreement 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 Agreement, Provider retains the right to use and disclose aggregated and De-Identified Data in any manner. “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, entity or particular Record can be identified, such that it is no longer Personal Information as defined in Applicable Privacy Laws.

PRIVACY REPRESENTATIVE

Provider will appoint a Privacy Representative and such person will have sufficient authority to make decisions and execute documents on behalf of Provider as may be required from time to time for the administration of this Agreement. Provider shall promptly provide Client the name and contact details of its Privacy Representative and shall notify Client 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 anticipated Material Breach, including full particulars of such breach.

Provider will cooperate with Client in preventing the occurrence or recurrence of any breach of this Agreement 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 demonstrating that Provider is compliant with this Agreement, 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 Agreement, for a Material Breach.

DEFAULT & TERMINATION

Notwithstanding anything in the Agreement to the contrary, Provider and Client hereby agree that a Material Breach by Provider will give rise to a right on the part of Client to terminate the Agreement immediately upon written notice.

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 documents or other 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. If, for any reason, Provider fails to return or destroy any Record in accordance with this Section, Provider's obligations pursuant to this Agreement will continue in full force and effect.

GENERAL

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

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

Unless otherwise expressly provided in the Agreement, if a provision of this Agreement 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 Agreement 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 Agreement.

PERSONAL HEALTH INFORMATION PROTECTION ACT ("PHIPA")

Under PHIPA, personal information includes personal address, and, in some cases, College of Physicians and Surgeons of Ontario numbers.

Uses and Disclosures of Personal Health Information

Although Provider does not intend to use or disclose any personal information, in the provision of website hosting services and other managed information technology services, Provider may have access to such information. Provider will safeguard personal information it receives, and may not use that information for any purpose other than provision of Services to a healthcare organization.

Consent

By providing personal information to Provider, an 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 Provider.

Personal information is treated as private and confidential

Provider will keep personal information protected and secure by providing security safeguards that are appropriate to the sensitivity of the information. Providers will only keep personal information for as long as it is required for legal or business purposes. Although the healthcare provider makes every reasonable effort to protect personal information from unauthorized access, release, use, loss and theft, disclosure, alteration by third parties, copying or modification by 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 information will be protected against loss, misuse or alteration, and does not accept any liability for personal information submitted by patients, nor for patients' or third parties' use or misuse of personal information.

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 healthcare organization with a 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 Information Management Agreement 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 Agreement 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 Agreement;

"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 Agreement.

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.

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 Agreement, 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 Agreement 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 Agreement.

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.

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.