Effective January 3, 2024. This Data Processing Agreement supersedes and replaces all prior versions.

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.

The parties agree as follows:

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

a. DEFINITIONS

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

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

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

d. Limitations on Use and Disclosure. Provider is prohibited from using or disclosing Client Personal Information for any purpose other than the specific purpose of performing the Services specified in the Agreement, the permitted business purposes set under applicable law, and as required under applicable law. Provider hereby certifies that it understands the foregoing restriction and will comply with it in accordance with the requirements of applicable U.S. Data Protection Laws.

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

2. **Colorado Privacy Act.** This section documents the safeguard standards imposed to protect Client information subject to the Colorado Privacy Act (6-1-1301) ("CPA"). To the extent Provider's services constitute processing of personal information governed by CPA, these provisions shall apply.

Provider shall adhere to the instructions of the controller and assist the controller to meet its obligations under the CPA.

Taking into account the nature of processing and the information available to Provider, Provider shall assist the controller by:

a. taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 6-1-1306;

b. helping to meet the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to section 6-1-716; and

c. providing information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 6-1-1309.

Notwithstanding the instructions of the controller, Provider shall:

a. ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and
b. engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

Taking into account the context of processing, Provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between Provider and the controller to implement the measures.

Processing by Provider must be governed by a contract between the controller and Provider that is binding on both parties and that sets out:

a. the processing instructions to which the processor is bound, including the nature and purpose of the processing;
b. the type of personal data subject to the processing, and the duration of the processing; and
c. the following requirements:
    (i) at the choice of the controller, Provider shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(ii) (a) Provider shall make available to the controller all information necessary to demonstrate compliance with the obligations; and

(b) Provider shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, Provider may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at Provider's expense, an audit of the Provider's policies and technical and organizational measures in support of its obligations under the CPA using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable. Provider shall furnish a report of the audit to the controller upon request.

3. **Connecticut Privacy Act.** This section documents the safeguard standards imposed to protect Client information subject to the Connecticut SB 12-2 ("Conn Act"). To the extent Provider's services constitute processing of personal information governed by Conn Act, these provisions shall apply.

Provider shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under the Conn Act. Such assistance shall include:

a. taking into account the nature of processing and the information available to Provider, providing appropriate technical and organizational measures to fulfill the controller's obligation to respond to consumer rights requests;

b. taking into account the nature of processing and the information available to Provider, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of Provider's systems, in order to meet the controller's obligations; and

c. providing necessary information to enable the controller to conduct and document data protection assessments.

Provider shall have a written contract with the controller that will govern the Provider's data-processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that Provider:

a. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

b. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

c. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate Provider's compliance with the obligations

d. after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of Provider with respect to the personal data; and

e. allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of Provider's policies and technical and organizational measures in support of the

obligations of the Conn Act using an appropriate and accepted control standard or framework and assessment procedure for such assessments.

Provider shall provide a report of such assessment to the controller upon request.

For purposes of the Conn Act, the following definitions apply:

a. "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

b. "Controller" means an individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data.

c. "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

d. "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

e. "Processor" means an individual who, or legal entity that, processes personal data on behalf of a controller

4. New York SHIELD

Provider maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Provider's business; (b) the amount of resources available to Provider; (c) the type of information that Provider will store; and (d) the need for security and confidentiality of such information. The Security Exhibit may be updated by Provider from time-to-time.

Provider's security program is designed to:

- Protect the confidentiality, integrity, and availability of Customer Data or Professional Services Data in Provider's possession or control or to which Provider has access;
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data or Professional Services Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer Data or Professional Services Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data or Professional Services Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Provider may be regulated.

Without limiting the generality of the foregoing, Provider's security program includes:

1. **Security Awareness and Training**. A mandatory security awareness and training program for all members of Provider's workforce (including management), which includes:
   a) Training on how to implement and comply with its Information Security Program;

b) Promoting a culture of security awareness through periodic communications from senior management with employees.

2. **Access Controls**. Policies, procedures, and logical controls:
   a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
   b) To prevent those workforce members and others who should not have access from obtaining access; and
   c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. **Physical and Environmental Security**. Controls that provide reasonable assurance that access to physical servers at the production data center or the facility housing Provider's SFTP Server, if applicable, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. These controls include:
   a) Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;
   b) Camera surveillance systems at critical internal and external entry points to the data center;
   c) Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and
   d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

4. **Security Incident Procedures**. A security incident response plan that includes procedures to be followed in the event of any Security Breach. Such procedures include:
   a) Roles and responsibilities: formation of an internal incident response team with a response leader;
   b) Investigation: assessing the risk the incident poses and determining who may be affected;
   c) Communication: internal reporting as well as a notification process in the event of unauthorized disclosure of Customer Data or Professional Services Data;
   d) Recordkeeping: keeping a record of what was done and by whom to help in later analysis and possible legal action; and
   e) Audit: conducting and documenting root cause analysis and remediation plan.

5. **Contingency Planning**. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

   a) Data Backups: A policy for performing periodic backups of production file systems and databases or Professional Services Data on Provider's SFTP Server, as applicable, according to a defined schedule;
   b) Disaster Recovery: A formal disaster recovery plan for the production data center, including:
      i) Requirements for the disaster plan to be tested on a regular basis, currently twice a year; and
      ii) A documented executive summary of the Disaster Recovery testing, at least annually, which is available upon request to customers.
   c) Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

6. **Audit Controls**. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information.

7. **Data Integrity**. Policies and procedures to ensure the confidentiality, integrity, and availability of Customer Data or Professional Services Data and protect it from disclosure, improper alteration, or destruction.

8. **Storage and Transmission Security**. Security measures to guard against unauthorized access to Customer Data or Professional Services Data that is being transmitted over a public electronic communications network

or stored electronically. Such measures include requiring encryption of any Customer Data or Professional Services Data stored on desktops, laptops or other removable storage devices.

9. **Secure Disposal**. Policies and procedures regarding the secure disposal of tangible property containing Customer Data or Professional Services Data, taking into account available technology so that Customer Data or Professional Services Data cannot be practicably read or reconstructed.

10. **Assigned Security Responsibility**. Assigning responsibility for the development, implementation, and maintenance of its Information Security Program, including:
    a) Designating a security official with overall responsibility;
    b) Defining security roles and responsibilities for individuals with security responsibilities; and
    c) Designating a Security Council consisting of cross-functional management representatives to meet on a regular basis.

11. **Testing**. Regularly testing the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified.

12. **Monitoring**. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:
    a) Reviewing changes affecting systems handling authentication, authorization, and auditing;
    b) Reviewing privileged access to Provider production systems; and
    c) Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

13. **Change and Configuration Management**. Maintaining policies and procedures for managing changes Provider makes to production systems, applications, and databases. Such policies and procedures include:
    a) A process for documenting, testing and approving the patching and maintenance of the Service;
    b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and
    c) A process for Provider to utilize a third party to conduct web application-level security assessments. These assessments generally include testing, where applicable, for:
        i) Cross-site request forgery
        ii) Services scanning
        iii) Improper input handling (e.g., cross-site scripting, SQL injection, XML injection, cross-site flashing)
        iv) XML and SOAP attacks
        v) Weak session management
        vi) Data validation flaws and data model constraint inconsistencies
        vii) Insufficient authentication
        viii) Insufficient authorization

14. **Program Adjustments**. Provider monitors, evaluates, and adjusts, as appropriate, the security program in light of:
    a) Any relevant changes in technology and any internal or external threats to Provider or the Customer Data or Professional Services Data;
    b) Security and data privacy regulations applicable to Provider; and
    c) Provider's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

15. **Devices**. All laptop and desktop computing devices utilized by Provider and any subcontractors when accessing Customer Data or Professional Services Data:
    a) will be equipped with hard disk drive encryption;
    b) will have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and

c) shall maintain virus and malware detection and prevention software so as to remain on a supported release. This shall include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by supplier of such software.

Definitions

"Professional Services" means consulting or professional services provided to Customer under an agreement between the parties for the provision of consulting or professional services.

"**Professional Services Data**" means electronic data or information that is provided to Provider under a Professional Services engagement with Provider for the purpose of being input into the Provider Service, or Customer Data accessed within or extracted from the Customer's tenant to perform the Professional Services.

"**SFTP Server**" means a Secure File Transfer Protocol server or its successor provided and controlled by Provider to transfer the Professional Services Data between Customer and Provider for implementation purposes.

5. Virginia Privacy Act. This section documents the safeguard standards imposed to protect Client information subject to the Code of Virginia Section 59.1-579 ("VPA"). To the extent Provider's services constitute processing of personal information governed by VPA, these provisions shall apply:

.

a. This DPA sets forth instructions for the following:
- **i.** Provider may provide hosting services and will only process data that is deposited by Client into Provider's systems;
- **ii.** Provider will not use non-anonomyzed protected data for any of its own business purposes;
- **iii.** Any processing will be for a reasonable amount of time given the Services to be performed; and
- **iv.** Both Provider and Client have the right to adjust whether Client may deposit protected data into Provider's systems.

b. With respect to the protected data, Provider shall:
- **i.** Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
- **ii.** At the Client's direction, delete or return all protected data to the Client as requested at the end of the provision of services, unless retention of the protected data is required by law;
- **iii.** Upon the reasonable request of the Client, make available to the Client all information in its possession necessary to demonstrate the Provider's compliance with the obligations in this chapter;
- **iv.** Allow, and cooperate with, reasonable assessments by the Client the Client's designated assessor; alternatively, Provider may arrange for a qualified and independent assessor to conduct an assessment of the Provider's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. Provider shall provide a report of such assessment to the Client upon request; and
- **v.** Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the Provider with respect to the protected data.

6. PIPEDA - This 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.

7. 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.