

## **MASTER SERVICES AGREEMENT**

### **AI-Powered Healthcare Services**

*Governing Law: Province of Ontario, Canada — Dispute Resolution: Toronto, Ontario*

This Master Services Agreement ("Agreement") is entered into as of the date of electronic acceptance ("Effective Date") by and between:

**Provider:** 2771764 Ontario Inc., carrying on business as Ample AI, with its principal place of business at 1065 Canadian Pl Ste 201 #332, Mississauga, ON L4W 0C2 ("Provider"); and

**Client:** The healthcare practice, clinic, or organization that accepts this Agreement by completing electronic checkout or by using the Services ("Client").

Provider and Client may each be referred to individually as a "Party" and collectively as the "Parties."

---

### **RECITALS**

**WHEREAS**, Provider is in the business of developing, deploying, and managing AI-powered services for healthcare practices, including virtual receptionist and call handling, workflow automation, clinic operations automation, and related technology solutions;

**WHEREAS**, Client operates a medical clinic or healthcare practice and desires to engage Provider to furnish such services;

**WHEREAS**, the Parties wish to set forth the terms governing the provision, use, and management of such services, including matters of data privacy, regulatory compliance, intellectual property, liability, and indemnification; and

**NOW, THEREFORE**, in consideration of the mutual covenants and agreements contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

---

### **ARTICLE 1 — DEFINITIONS**

**1.1** "AI System" means Provider's proprietary artificial intelligence software platform and all automation tools used to deliver the Services, including underlying algorithms, machine learning models, natural language processing engines, voice synthesis technology, workflow automation engines, task orchestration tools, clinic operations automation modules, third-party integrations, APIs, and related technology components.

**1.2** "Authorized Users" means Client's employees, regulated health professionals, contractors, agents, and staff members authorized by Client to access and use the Services.

**1.3** "Client Data" means all data, information, records, and materials provided by Client or its patients to Provider or input into the AI System in connection with the Services, including patient information, appointment records, scheduling data, and any other information transmitted through or stored within the AI System. Client Data includes Health Data.

**1.4** "Confidential Information" means any non-public, proprietary, or confidential information disclosed by one Party to the other, whether in written, oral, or electronic form, including trade secrets, business plans, financial information, pricing, customer lists, Health Data, technical specifications, source code, algorithms, and marketing strategies.

**1.5** "Data Protection Addendum" or "DPA" means the applicable exhibit attached to this Agreement governing the collection, use, disclosure, and protection of Health Data, as determined by Client's jurisdiction of operation pursuant to Article 7.

**1.6** "Documentation" means all user manuals, training materials, technical specifications, integration guides, and other written or electronic materials provided by Provider to Client in connection with the Services.

**1.7** "Effective Date" means the date on which Client accepts this Agreement by electronic checkout or first uses the Services, whichever is earlier.

**1.8** "Health Data" means all personal health information, personal information, or protected health information (as those terms are defined under the laws applicable to Client's jurisdiction) collected, used, disclosed, or otherwise processed by Provider on behalf of Client in connection with the Services, as further described in the applicable DPA.

**1.9** "Intellectual Property" means all patents, copyrights, trademarks, trade secrets, know-how, inventions, algorithms, models, software, source code, object code, designs, processes, and any other intellectual property rights, whether registered or unregistered.

**1.10** "Order Form" or "Service Order" means any written or electronic order form, statement of work, or service schedule executed by both Parties (or accepted electronically at checkout) that references this Agreement and sets forth the specific Services, fees, service levels, and other terms applicable to a particular engagement.

**1.11** "Permitted Purpose" means the use of the Services solely for Client's internal business operations, including the administration, management, and automation of clinical and operational workflows within Client's healthcare practice.

**1.12** "Services" means the AI-powered services provided by Provider to Client as described in this Agreement and any applicable Order Form, which may include any combination of: (a) AI receptionist and virtual call handling (inbound and outbound); (b) automated appointment scheduling, confirmations, and reminders; (c) patient intake processing and routing; (d) after-hours call management and message taking; (e) insurance verification assistance; (f) prescription refill request routing; (g) recall and waitlist management; (h) workflow and clinic operations automation, including task routing, staff notifications, EHR/PMS integrations, and process automation between third-party platforms; (i) custom automation builds; and (j) any additional services mutually agreed in writing.

**1.13** "Term" has the meaning set forth in Article 5.

**1.14** "Third-Party Components" means any software, services, APIs, platforms, or tools owned or controlled by third parties that are integrated with or used in connection with the AI System.

## ARTICLE 2 — SCOPE OF SERVICES

**2.1 Delivery.** Provider shall deliver the Services as described in the applicable Service Order, which may include AI receptionist and virtual call handling, workflow and clinic operations automation, EHR/PMS and third-party platform integrations, custom automation builds, and related services. Provider reserves the right to update or modify the Services at any time, provided that such changes do not materially reduce core functionality described in the applicable Service Order without Client's prior written consent.

**2.2 Training.** Provider shall provide initial training to Client's Authorized Users as described in the applicable Service Order. Additional training beyond the initial scope may be subject to additional fees as set out in a supplementary Order Form.

**2.3 Escalation Protocols.** The Parties shall establish escalation procedures for matters requiring human intervention, as set forth in the applicable Service Order. Provider shall route escalated matters to Client's designated staff in accordance with those procedures.

**2.4 AI Disclosure.** Client is solely responsible for determining and implementing any verbal, written, visual, or script-based disclosures required under applicable laws and regulations regarding AI-assisted interactions, automated communications, or consumer transparency in Client's jurisdiction. At Client's direction, Provider may configure or operationalize disclosures, notices, and consent language provided, approved, or confirmed by Client, but Provider is not responsible for independently determining the sufficiency of such disclosures for Client's particular legal or operational requirements.

**2.5 No Medical Advice.** The Services are administrative technology tools and do not constitute medical advice, diagnosis, or treatment. Client is solely responsible for all clinical decisions.

**2.6 Emergency and High-Risk Use.** THE SERVICES ARE NOT EMERGENCY RESPONSE SERVICES, ARE NOT MONITORED FOR 911, 988, OR OTHER URGENT COMMUNICATIONS, AND ARE NOT A SUBSTITUTE FOR STAFFED PHONE LINES, CLINICAL TRIAGE, OR LEGALLY REQUIRED PATIENT MONITORING. CLIENT SHALL NOT USE THE SERVICES AS ITS SOLE MECHANISM FOR RECEIVING OR RESPONDING TO EMERGENCIES, TIME-CRITICAL CLINICAL COMMUNICATIONS, OR OTHER HIGH-RISK MATTERS.

**2.7 Suspension for Security or Legal Risk.** Provider may suspend or restrict the Services immediately, in whole or in part, to the minimum extent reasonably necessary if Provider reasonably believes that use of the Services poses a security risk, violates applicable law, threatens the rights, safety, or data of any person, or could expose Provider or its subprocessors to material liability. Provider shall provide prompt notice of any such suspension and restore the affected Services as soon as reasonably practicable.

---

## ARTICLE 3 — CLIENT OBLIGATIONS

**3.1 Cooperation.** Client shall cooperate with Provider in good faith and provide such information, access, and assistance as Provider reasonably requires to perform the Services, including:

- (a) Timely provision of accurate practice information, scheduling rules, provider availability, and workflow specifications;

- (b) Access to Client's EHR, PMS, phone systems, and other relevant platforms necessary for integration;
- (c) Designation of a primary point of contact and project liaison; and
- (d) Timely review, feedback, and approval of configurations and workflows.

**3.2 Accuracy of Information.** Client is solely responsible for the accuracy, completeness, and timeliness of all information, data, and instructions provided to Provider for configuration of the AI System. Provider shall not be liable for errors or adverse outcomes resulting from inaccurate, incomplete, or outdated information provided by Client.

**3.3 Patient Consent.** Client is solely responsible for obtaining, documenting, and maintaining all patient consents, authorizations, opt-ins, acknowledgements, and privacy notices required under applicable law, including consents and notices relating to automated communications, AI interactions, call recording, cross-border processing, and the collection, use, disclosure, or transfer of Health Data.

**3.4 Acceptable Use.** Client shall not, and shall ensure that its Authorized Users do not: (a) use the Services for any unlawful purpose; (b) reverse engineer, decompile, or disassemble the AI System; (c) sublicense or resell the Services without Provider's prior written consent; (d) interfere with or disrupt the integrity or performance of the Services; or (e) use the Services in any manner that violates applicable law or this Agreement.

**3.5 Human Oversight.** Client shall maintain adequate staffing to handle escalated matters, medical emergencies, and situations requiring human judgment. Provider is not liable for harm arising from Client's failure to maintain such oversight.

**3.6 Regulatory Compliance.** Client shall comply with all applicable laws in connection with its use of the Services, including applicable privacy laws, telehealth regulations, recording consent laws, and consumer protection legislation in Client's jurisdiction.

**3.7 Messaging and Calling Compliance.** Client is solely responsible for determining the lawful basis for, and obtaining and maintaining, all consents, authorizations, notices, opt-ins, and opt-out processes required for calls, SMS/MMS, prerecorded or artificial voice communications, emails, faxes, and similar communications sent or placed through the Services, including under CASL, TCPA, CAN-SPAM, state mini-TCPA laws, and applicable call recording or wiretapping laws. Client shall maintain evidence of such consents and suppression preferences and shall promptly provide Provider with any updates needed to honor them.

**3.8 Emergency Routing and Fallback Procedures.** Client shall maintain documented emergency routing, after-hours coverage, and business continuity procedures, including staffed fallback channels if the Services or any Third-Party Components are unavailable. Provider is not responsible for emergency escalation failures caused by Client's failure to maintain such procedures.

**3.9 Configuration Approval and Monitoring.** Client is responsible for reviewing and approving workflows, prompts, scripts, routing rules, booking logic, escalation paths, FAQs, automated messages, consent language, and any other Client-specific configuration before production use and after any material change. Client shall monitor outputs and promptly notify Provider of any suspected error, misrouting, unsafe response, non-compliant communication, or needed update to approved scripts, notices, consent language, or escalation logic.

**3.10 Material Changes in Usage Profile.** Client shall promptly notify Provider if Client reasonably expects or becomes aware of any material increase in locations, providers, operating hours, call volume,

connected minutes, messaging volume, supported workflows, or other usage characteristics that may affect pricing, technical configuration, or support requirements.

3.11 Special Data Restrictions and Segmentation. Client shall identify to Provider in writing any lock-box directive, segmented record requirement, masking rule, special confidentiality flag, redisclosure restriction, or similar limitation applicable to data handled through the Services, and Provider shall have no responsibility for implementing or honoring any such restriction unless and until it is clearly communicated by Client and expressly supported in the agreed configuration.

---

## ARTICLE 4 — FEES AND PAYMENT

**4.1 Fees.** In consideration of the Services, Client shall pay Provider the following fees ("Fees"):

**(a) Integration Fee.** A one-time integration and setup fee as specified in the applicable Order Form (the "Integration Fee"), which is earned by Provider upon execution of this Agreement. The Integration Fee is non-refundable and represents compensation for configuration, onboarding, and deployment costs incurred prior to or at commencement of Service delivery. Client agrees not to initiate any payment reversal or dispute with respect to the Integration Fee except in the event of Provider's material breach of this Agreement.

**(b) Monthly or Other Recurring Service Fees.** The recurring service fees specified in the applicable Order Form or Service Order (collectively, the "Recurring Fees") are due and payable in advance at the start of each applicable billing period unless the Service Order expressly provides a different billing schedule. Unless otherwise stated in the applicable Service Order, monthly Recurring Fees are due on the Effective Date and every thirty (30) days thereafter, and annual or other fixed-term Recurring Fees are due on the Effective Date and on each renewal date thereafter. Recurring Fees are non-refundable once the applicable billing period has commenced.

**(c) Additional Fees.** Any fees for services or customizations outside the standard scope shall be as set forth in a supplementary Order Form or as mutually agreed in writing prior to the commencement of such services.

**(d) Pricing Basis and Package Assumptions.** Fees, tiers, included usage, and any discounted pricing stated in the applicable Service Order are based on the clinic profile and commercial assumptions identified by Provider, which may include clinic size, number of locations, number of providers, expected inbound and outbound call volume, connected minutes, messaging volume, after-hours coverage, integrations, and support scope.

**(e) Overage Fees; Re-tiering.** If Client's actual usage exceeds any included usage or other assumptions reflected in the applicable Service Order, Provider may bill applicable overage, usage-based, telecommunications, messaging, carrier, or third-party pass-through fees at the rates stated in the applicable Service Order, or if no such rates are stated, at Provider's then-current standard rates on prior written notice. If Client's usage materially exceeds the assumptions underlying the agreed pricing for two (2) consecutive billing cycles or for any three (3) billing cycles in a rolling four (4) month period, Provider may re-tier the Services or require an amended Service Order on thirty (30) days' prior written notice.

**4.2 Payment Authorization.** Provider shall issue invoices for Recurring Fees no later than five (5) business days prior to each due date, or for the initial billing period on or promptly after the Effective

Date, unless the applicable Service Order provides otherwise. Client shall maintain valid payment information on file. For credit card payments, Provider currently uses Stripe as its third-party payment processor and may change processors on notice to Client. Client authorizes Provider and its payment processor to store applicable payment credentials using tokenized or processor-hosted methods and to charge, retry, and recover Recurring Fees, usage-based charges, overages, taxes, pass-through charges, chargeback fees, and other amounts owed under this Agreement on each due date or as otherwise provided in the applicable Service Order. Client acknowledges that Provider does not store full payment card numbers where Stripe-hosted or equivalent processor-hosted collection is used.

**4.3 Late Payments.** Overdue amounts shall accrue interest at the rate of one and one-half percent (1.5%) per month (eighteen percent (18%) per annum), or the maximum rate permitted by applicable law, whichever is less, calculated from the due date until paid in full. All amounts owed under this Agreement are payable without setoff, withholding, counterclaim, deduction, or abatement except as required by applicable law. If any automatic payment fails, is declined, expires, is reversed, or becomes invalid, Client remains responsible for timely payment and shall promptly provide an updated payment method. If Client initiates a chargeback, retrieval request, or payment dispute for a charge not caused by Provider's material breach, Client remains liable for the underlying amount and shall reimburse Provider for reasonable processor fees, external collection costs, and reasonable attorneys' fees incurred in responding to or reversing the dispute. Provider may suspend Services upon fifteen (15) days' prior written notice if any undisputed amount remains unpaid after its due date or if Client fails to update invalid payment information within five (5) business days after notice.

**4.4 Taxes.** All fees are exclusive of applicable taxes. Client is responsible for all sales, use, GST, HST, or similar taxes arising from this Agreement, excluding taxes on Provider's net income.

**4.5 Fee Adjustments.** Provider may adjust fees on not less than sixty (60) days' prior written notice, effective at the start of any renewal term. Fee increases during the Initial Term shall not exceed five percent (5%) per annum unless otherwise specified in the Service Order.

**4.6 Disputed Invoices.** If Client disputes any portion of an invoice in good faith, Client shall: (a) pay the undisputed portion by the due date; (b) provide written notice of the dispute with supporting detail within fifteen (15) days of receipt of the invoice; and (c) cooperate with Provider to resolve the dispute. Failure to dispute an invoice within fifteen (15) days of receipt constitutes acceptance of the invoice in full.

**4.7 Refunds.** Unless otherwise required by applicable law or expressly provided herein, all fees are non-refundable once the applicable billing period has commenced. The Integration Fee is non-refundable once onboarding, configuration, or implementation work begins, or as of the Effective Date if earlier. Recurring fees are billed in advance unless the applicable Service Order expressly provides otherwise. For annual or other fixed-term plans, all recurring fees committed for the then-current fixed term are non-cancellable and non-refundable once that fixed term begins, and any installment schedule is a payment accommodation only and does not reduce Client's commitment for the full fixed term. Usage-based charges, overages, telecommunications charges, messaging charges, carrier charges, third-party pass-through charges, taxes, and other accrued amounts remain payable notwithstanding cancellation, suspension, or termination.

---

## ARTICLE 5 — TERM AND TERMINATION

**5.1 Term.** This Agreement commences on the Effective Date and continues for the initial term specified in the applicable Service Order (the "Initial Term"). Where the Service Order specifies a

**fixed-term arrangement, including an annual plan or any other committed term, the Agreement continues for that fixed term and renews automatically for successive terms of the same length (or, for annual plans, successive twelve (12) month periods) unless either Party provides written notice of non-renewal no later than sixty (60) days before the end of the then-current term. Any purported notice of non-renewal or cancellation delivered less than sixty (60) days before the end of a then-current annual or other fixed term is ineffective to prevent that renewal and shall instead apply to the end of the following renewal term unless Provider agrees otherwise in writing. Where the Service Order specifies a month-to-month arrangement, the Agreement continues on a rolling monthly basis until terminated in accordance with Section 5.3.**

5.2 Cancellation Window. Client may cancel this Agreement for any reason within the first thirty (30) calendar days following the Effective Date by providing written notice to Provider. If Client exercises this right: (a) the Agreement terminates on the date Provider receives such notice; (b) all Recurring Fees already invoiced or attributable to any billing period that has commenced, together with any accrued usage-based charges, overages, telecommunications charges, messaging charges, carrier charges, third-party pass-through charges, taxes, and other amounts incurred through the effective date of cancellation, remain due and payable and, to the extent already charged for a commenced billing period, are non-refundable; (c) the Integration Fee remains non-refundable; and (d) no early termination fee applies. This right is available only once, regardless of billing arrangement.

**5.3 Termination for Convenience. After expiration of the Cancellation Window set out in Section 5.2: (a) if Client is on a fixed-term arrangement, including an annual plan whether prepaid or paid in installments, either Party may elect non-renewal effective at the end of the then-current fixed term only by timely notice under Section 5.1. Unless the applicable Service Order expressly provides otherwise, a convenience termination notice given during a fixed term does not shorten the then-current term. If Client terminates, ceases using the Services, or requests cancellation during the then-current fixed term, Client remains liable for all Fees committed for that fixed term, including any unpaid installments, accrued usage-based charges, overages, telecommunications charges, messaging charges, carrier charges, third-party pass-through charges, taxes, and any applicable early termination fee set out in the Service Order; if no different early termination fee is stated in the Service Order, the early termination fee shall equal the lesser of (i) the remaining recurring Fees for the balance of the fixed term or (ii) three (3) months of recurring Fees at the then-current rate; and (b) if Client is on a month-to-month arrangement as specified in the Service Order, either Party may terminate on thirty (30) days' prior written notice, effective at the end of the then-current billing cycle or the end of the notice period, whichever is later, and no early termination fee applies.**

5.4 Termination for Cause. Either Party may terminate this Agreement immediately on written notice if the other Party: (a) commits a material breach and fails to cure within thirty (30) days of written notice describing the breach in reasonable detail (ten (10) days for payment breaches); (b) becomes insolvent, makes an assignment for the benefit of creditors, files for or has filed against it a petition in bankruptcy or receivership, or ceases operations; or (c) commits a material violation of any applicable privacy or data protection law that is not cured within the timeframe required by such law.

5.5 Effect of Termination. On termination or expiration of this Agreement for any reason: (a) Provider shall cease providing the Services and shall terminate Client's access to the AI System; (b) all accrued and unpaid fees become immediately due and payable; (c) Provider shall make Client Data available for export for thirty (30) days following the effective date of termination, after which Provider shall have no obligation to retain Client Data; (d) each Party shall return or destroy the other Party's Confidential Information in accordance with Article 11; (e) Provider shall return or securely destroy all Health Data in accordance with the applicable DPA; and (f) the following provisions shall survive termination or

expiration: Articles 1, 4 (with respect to fees accrued prior to the effective date of termination), 6, 8.4, 9, 10, 11, 12, and 13.

**5.6 Transition Assistance.** If Client requests transition or migration assistance within thirty (30) days following termination or expiration, Provider may provide reasonable assistance at Provider's then-current professional services rates, subject to technical feasibility, the Parties' mutual scheduling availability, and payment of all undisputed amounts due under this Agreement.

---

## ARTICLE 6 — INTELLECTUAL PROPERTY

**6.1 Provider IP.** Provider retains all right, title, and interest in and to the Services, including all software, AI models, algorithms, workflows, templates, know-how, Documentation, and all improvements, modifications, and derivative works thereof. Nothing in this Agreement transfers ownership of Provider's Intellectual Property to Client.

**6.2 Client Data.** Client retains all right, title, and interest in and to Client Data, including all Health Data. Provider acquires no ownership interest in Client Data by virtue of this Agreement.

**6.3 License Grant.** Provider grants Client a limited, non-exclusive, non-transferable, revocable license to access and use the Services during the Term solely for the Permitted Purpose.

**6.4 Feedback.** If Client provides Provider with suggestions, feedback, or recommendations regarding the Services ("Feedback"), Client hereby assigns to Provider all right, title, and interest in and to such Feedback. Provider may use Feedback without restriction or compensation to Client, provided such Feedback does not contain Health Data.

**6.5 No AI Training Without Consent.** Provider shall not use Client Data or Health Data to train or improve AI models for purposes unrelated to the direct provision of Services to Client, unless Client has provided express prior written consent. Provider shall not sell or otherwise commercialize Client Data or Health Data to any third party.

**6.6 De-Identified Data.** Notwithstanding Section 6.5, Provider may create, use, and disclose de-identified and aggregated statistical data derived from Client Data, provided: (a) de-identification is performed using methods that meet the applicable standard under Client's jurisdiction (including, as applicable, 45 CFR § 164.514 for US clients and PHIPA de-identification guidelines for Ontario clients); (b) the resulting data cannot reasonably identify any individual, Client, or its patients; and (c) such use is limited to Provider's internal analytics and product improvement. Provider shall not attempt to re-identify any de-identified data. Client may opt out of such use on thirty (30) days' written notice.

**6.7 Trademarks.** Neither Party shall use the other's name, logo, or trademarks without prior written consent, except that Provider may reference Client's name in its customer list and marketing materials, subject to Client's right to opt out on thirty (30) days' written notice.

**6.8 Restrictions.** Except as expressly permitted herein, Client shall not: (a) copy, modify, or create derivative works of the AI System, Services, or Documentation; (b) reverse engineer, decompile, or disassemble the AI System; (c) rent, lease, sell, or sublicense the Services; (d) remove or alter any proprietary notices from the Services or Documentation; or (e) use the Services to develop a substantially similar or competing product.

## ARTICLE 7 — DATA PROTECTION

7.1 **Applicable Data Protection Addendum.** The collection, use, disclosure, and protection of Health Data processed by Provider on behalf of Client under this Ontario form is governed by Exhibit B — Ontario PHIPA Service Provider Privacy Agreement, which is attached hereto and incorporated by reference.

7.2 **Conflict.** In the event of any conflict between this Agreement and the applicable DPA with respect to the handling, protection, or privacy of Health Data, the DPA shall control.

7.3 **Multiple Jurisdictions.** If Client operates in multiple jurisdictions each subject to a different DPA, Client shall notify Provider in writing at the time of signing. The Parties shall cooperate to identify and execute all applicable DPAs. Each executed DPA is incorporated into this Agreement by reference.

7.4 **Minimum Security Baseline.** Regardless of the applicable DPA, Provider shall at all times maintain: (a) encryption of Health Data at rest (AES-256 or equivalent) and in transit (TLS 1.2 or higher); (b) role-based access controls limiting access to authorized personnel; (c) multi-factor authentication for all systems processing Health Data; (d) audit logging of all access, uses, and modifications of Health Data; (e) regular vulnerability assessments and penetration testing; (f) documented incident response and data breach response procedures; and (g) a designated Privacy Officer and Security Officer.

7.5 **Subprocessors.** Provider shall maintain a current list of subprocessors and third-party service providers that process Health Data on its behalf. Provider shall make this list available to Client upon written request and shall notify Client of any material changes to its subprocessor list at least thirty (30) days in advance.

7.6 **Cross-Border Processing and Third-Party Infrastructure.** Client acknowledges that Provider and its subprocessors may process Client Data in Canada, the United States, or other jurisdictions disclosed in Provider's subprocessor documentation or agreed service architecture. Where data is transferred across borders, Provider shall use contractual and operational measures designed to provide the level of protection required by applicable law. Client remains responsible for making any notices or disclosures to patients, callers, or other individuals required by applicable law in connection with such cross-border processing, and represents and warrants that it has provided, and will maintain, all required notices, disclosures, and consents for the use of Provider and its disclosed subprocessors as service providers in such jurisdictions.

7.7 **Security Incident Cooperation.** In addition to obligations under the applicable DPA, each Party shall promptly notify the other of any security incident reasonably likely to materially affect the Services or Client Data and shall cooperate in good faith in containment, investigation, remediation, and legally required notices.

7.8 **Audit Evidence.** No more than once in any twelve (12) month period, upon reasonable written request, Provider shall make available summary information reasonably demonstrating its compliance with the security commitments in this Agreement, such as relevant policies, certifications, or third-party assessment summaries, subject to confidentiality restrictions. Any on-site audit, penetration testing, or

other intrusive review requires Provider's prior written consent and may be subject to mutually agreed scope, security controls, scheduling, and reimbursement of Provider's reasonable costs.

**7.9 Additional Regulatory Regimes.** Client shall notify Provider in writing before transmitting data subject to any law or regime imposing obligations materially beyond those expressly addressed in this Agreement or the applicable DPA, including 42 CFR Part 2, court sealing obligations, lock-box or segmentation requirements, or similar enhanced confidentiality rules. Unless the Parties expressly agree in writing to additional controls, the Services are not represented as configured for such heightened requirements, and Provider may decline, limit, or suspend the affected Services to the minimum extent reasonably necessary where supporting such jurisdiction, regime, or restriction would require materially different technical, contractual, or operational controls than those reflected in this Agreement.

---

## ARTICLE 8 — REPRESENTATIONS AND WARRANTIES

**8.1 Mutual Representations.** Each Party represents and warrants that: (a) it is duly organized, validly existing, and in good standing under the laws of its jurisdiction of formation or incorporation; (b) it has full power and authority to enter into and perform its obligations under this Agreement; (c) the execution and performance of this Agreement does not conflict with or violate any other agreement to which it is a party or by which it is bound; and (d) it shall comply with all applicable laws in the performance of its obligations under this Agreement.

**8.2 Provider Representations.** Provider represents and warrants that: (a) the Services shall be performed in a professional and workmanlike manner consistent with generally accepted industry standards; (b) the Services shall materially conform to the specifications in the applicable Order Form and Documentation; (c) Provider holds all licences and certifications required to provide the Services in the applicable jurisdiction; (d) to Provider's knowledge as of the Effective Date, the AI System does not infringe any third party's Intellectual Property rights; (e) Provider shall maintain the minimum security baseline described in Section 7.4 at all times; (f) Provider shall comply with all applicable privacy and data protection laws in its handling of Health Data; and (g) all personnel with access to Health Data shall have received appropriate privacy and security training prior to such access.

**8.3 Client Representations.** Client represents and warrants that: (a) Client holds all licences and certifications required to operate its medical or healthcare practice; (b) Client shall obtain all patient consents, authorizations, and notices required by applicable law prior to providing Health Data to Provider; (c) all information, scripts, workflows, and instructions provided by Client to Provider are, to Client's knowledge, accurate, complete, and lawfully provided; (d) Client shall use the Services solely for the Permitted Purpose; (e) Client has provided, and will maintain, any privacy notices or disclosures required to identify or describe Provider and its subprocessors as service providers or processors, including for cross-border processing where applicable; and (f) Client shall promptly notify Provider of any lock-box, segmentation, masking, suppression, or other special confidentiality restriction applicable to data handled through the Services.

**8.4 DISCLAIMER OF WARRANTIES.** EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN ARTICLE 8, THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." PROVIDER DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. PROVIDER DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR FREE FROM HARMFUL COMPONENTS, OR THAT AI-GENERATED OUTPUT WILL BE ACCURATE, COMPLETE, OR

SUITABLE FOR ANY PARTICULAR PURPOSE. NOTHING IN THIS SECTION 8.4 LIMITS PROVIDER'S OBLIGATIONS UNDER THE APPLICABLE DPA OR APPLICABLE PRIVACY LAW.

**8.5 Compliance Dependency.** Client acknowledges that legal and operational compliance for any workflow depends materially on Client's instructions, consent practices, staffing, approved scripts, configuration, jurisdiction-specific obligations, and the third-party systems selected by Client. Except as expressly set out in this Agreement or the applicable DPA, Provider does not warrant that Client's particular implementation or use of the Services will satisfy all laws applicable to Client.

---

## ARTICLE 9 — LIMITATION OF LIABILITY

9.1 EXCLUSION OF INDIRECT DAMAGES. EXCEPT FOR A PARTY'S OBLIGATIONS UNDER ARTICLE 10 (INDEMNIFICATION), BREACH OF ARTICLE 7 (DATA PROTECTION) OR THE APPLICABLE DPA, BREACH OF ARTICLE 11 (CONFIDENTIALITY), OR A PARTY'S GROSS NEGLIGENCE OR WILFUL MISCONDUCT, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES, INCLUDING LOSS OF PROFITS, REVENUE, DATA, GOODWILL, OR ANTICIPATED SAVINGS, REGARDLESS OF THE THEORY OF LIABILITY AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9.2 AGGREGATE LIABILITY CAP. EXCEPT FOR A PARTY'S OBLIGATIONS UNDER ARTICLE 10, BREACH OF ARTICLE 7 OR THE APPLICABLE DPA, INFRINGEMENT OF A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS, BREACH OF ARTICLE 11, OR A PARTY'S GROSS NEGLIGENCE OR WILFUL MISCONDUCT, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE TOTAL FEES PAID OR PAYABLE BY CLIENT TO PROVIDER IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

9.3 ELEVATED CAP. FOR CLAIMS ARISING FROM BREACH OF ARTICLE 7 OR THE APPLICABLE DPA (DATA PROTECTION), ARTICLE 11 (CONFIDENTIALITY), OR INFRINGEMENT OF A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS, EACH PARTY'S TOTAL AGGREGATE LIABILITY SHALL NOT EXCEED TWO TIMES (2×) THE TOTAL FEES PAID OR PAYABLE BY CLIENT TO PROVIDER IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

9.4 EXCLUSIONS FROM CAPS. THE LIMITATIONS IN SECTIONS 9.1, 9.2, AND 9.3 DO NOT APPLY TO: (A) GROSS NEGLIGENCE OR WILFUL MISCONDUCT; (B) INDEMNIFICATION OBLIGATIONS UNDER ARTICLE 10; (C) CLIENT'S OBLIGATION TO PAY FEES DUE UNDER THIS AGREEMENT; (D) REGULATORY FINES OR PENALTIES IMPOSED AS A DIRECT RESULT OF A PARTY'S OWN BREACH OF APPLICABLE LAW; OR (E) LIABILITY THAT CANNOT BE LIMITED OR EXCLUDED UNDER APPLICABLE LAW.

9.5 AI TECHNOLOGY RISK. THE AI SYSTEM UTILIZES MACHINE LEARNING TECHNOLOGIES THAT MAY PRODUCE OUTPUTS THAT ARE INACCURATE, INCOMPLETE, OR CONTEXTUALLY INAPPROPRIATE. PROVIDER SHALL NOT BE LIABLE FOR DAMAGES ARISING FROM: (A) THE INHERENT TECHNICAL LIMITATIONS OF AI-GENERATED CONTENT; (B) DECISIONS MADE BY CLIENT, ITS STAFF, OR ITS PATIENTS IN RELIANCE ON AI-GENERATED CONTENT WITHOUT APPROPRIATE HUMAN REVIEW; OR (C) CLIENT'S FAILURE TO COMPLY WITH ITS OBLIGATIONS UNDER THIS AGREEMENT. THE FEES

CHARGED UNDER THIS AGREEMENT REFLECT THE ALLOCATION OF RISK SET FORTH IN THIS ARTICLE 9.

**9.6 Payment Obligations.** Nothing in this Article 9 limits Client's obligation to pay all fees due and payable under this Agreement.

**9.7 Third-Party Platforms and Carriers.** Provider is not responsible for delays, delivery failures, message filtering, spam blocking, caller-ID labeling, telecom or carrier restrictions, API outages, calendar conflicts, EHR/PMS errors, payment processor outages, fraud screening decisions, reserves, holds, payout delays, or other issues caused by Third-Party Components, payment processors (including Stripe), telecommunications carriers, internet service providers, or Client systems, except to the extent caused by Provider's breach of this Agreement.

---

## ARTICLE 10 — INDEMNIFICATION

**10.1 Provider Indemnity.** Provider shall defend, indemnify, and hold harmless Client and its officers, directors, employees, and agents ("Client Indemnitees") from and against any and all third-party claims, losses, damages, liabilities, and expenses (including reasonable attorneys' fees) ("Losses") arising from or related to: (a) Provider's material breach of this Agreement; (b) Provider's gross negligence or wilful misconduct; (c) any unauthorized access to or disclosure of Health Data caused by Provider's acts or omissions; (d) Provider's material violation of applicable law; or (e) a third-party allegation that the AI System, as provided by Provider and used by Client in strict accordance with this Agreement, infringes a third party's Intellectual Property rights.

**10.2 Client Indemnity.** Client shall defend, indemnify, and hold harmless Provider and its officers, directors, employees, and agents ("Provider Indemnitees") from and against any and all Losses arising from or related to: (a) Client's material breach of this Agreement; (b) Client's gross negligence or wilful misconduct; (c) Client's failure to obtain required patient consents or authorizations; (d) Client's use of the Services in violation of applicable law; (e) any claim arising from Client's failure to maintain adequate human oversight of the Services or to follow established escalation protocols; (f) Client's provision of inaccurate or misleading information to Provider; (g) any claim relating to the practice of medicine or clinical decision-making by Client or its staff; (h) any claim, investigation, fine, penalty, carrier enforcement action, or similar proceeding arising from Client's failure to obtain or honor required consents, opt-outs, notices, or recording disclosures for communications sent or placed through the Services; (i) any content, scripts, FAQs, pricing, clinical instructions, routing criteria, or other materials supplied, approved, or required by Client; or (j) Client's use of the Services for emergency, diagnostic, treatment, or other high-risk purposes not expressly authorized under this Agreement.

**10.3 IP Infringement Remedies.** If the Services become the subject of an intellectual property infringement claim, Provider may, at its sole option and expense: (a) procure for Client the right to continue using the Services; (b) modify the Services to be non-infringing without materially reducing core functionality; or (c) if neither (a) nor (b) is commercially practicable, terminate the affected Services and refund any prepaid, unused fees for the remainder of the then-current term.

**10.4 Breach Response Costs.** The Party whose act or omission caused or materially contributed to a data breach or privacy incident shall bear the reasonable and direct costs of breach response, including notifications, forensic investigation, credit monitoring (where required by law), and regulatory communications. Where causation is shared or disputed, the Parties shall cooperate in good faith to allocate costs proportionally.

**10.5 Indemnification Procedures.** The indemnified party shall: (a) provide prompt written notice of any claim for which indemnification is sought; (b) grant the indemnifying party sole control of the defense and settlement, provided that the indemnified party may participate at its own expense with counsel of its choice; and (c) provide reasonable cooperation at the indemnifying party's expense. The indemnifying party shall not settle any claim on terms that impose liability, obligations, or restrictions on the indemnified party without its prior written consent.

---

## ARTICLE 11 — CONFIDENTIALITY

**11.1 Obligations.** Each Party (as "Receiving Party") shall: (a) hold the other Party's Confidential Information in strict confidence; (b) not disclose it to any third party except as permitted under this Article 11; (c) use it solely for the purposes of performing or receiving the Services under this Agreement; and (d) protect it using at least the same degree of care as it uses to protect its own confidential information of similar sensitivity, but in no event less than reasonable care.

**11.2 Permitted Disclosures.** The Receiving Party may disclose Confidential Information to its employees, contractors, and professional advisors who have a genuine need to know such information and who are bound by written confidentiality obligations no less restrictive than those in this Article 11. The Receiving Party remains fully responsible for any breach of this Article 11 by such persons.

**11.3 Exclusions.** The obligations in Section 11.1 do not apply to information that: (a) is or becomes publicly available through no act or omission of the Receiving Party; (b) was rightfully known to the Receiving Party prior to disclosure without restriction; (c) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information; or (d) is rightfully received from a third party without any restriction on disclosure.

**11.4 Compelled Disclosure.** If the Receiving Party is required by applicable law, regulation, or governmental authority to disclose Confidential Information, it shall: (a) provide prompt prior written notice to the Disclosing Party to the extent permitted by law; (b) cooperate with the Disclosing Party in seeking a protective order or other appropriate relief; and (c) disclose only such Confidential Information as is legally required and use reasonable efforts to obtain confidential treatment for any information disclosed.

**11.5 Return or Destruction.** On termination of this Agreement or on written request by the Disclosing Party, the Receiving Party shall promptly return or destroy all Confidential Information in its possession or control and, on request, certify such return or destruction in writing. This obligation is subject to any applicable legal retention requirements.

**11.6 Duration.** Confidentiality obligations under this Article 11 survive termination or expiration of this Agreement for a period of five (5) years, except that: (a) obligations regarding trade secrets continue indefinitely for so long as such information constitutes a trade secret under applicable law; and (b) obligations regarding Health Data survive indefinitely or for such longer period as required by the applicable DPA or applicable law.

---

## ARTICLE 12 — DISPUTE RESOLUTION

**12.1 Negotiation.** Before initiating any formal proceeding, the Parties shall attempt to resolve any dispute, claim, or controversy arising out of or relating to this Agreement through good-faith

---

senior-executive negotiations. Either Party may initiate this process by providing written notice to the other Party identifying the dispute in reasonable detail. The Parties shall have thirty (30) days from the date of such notice to resolve the dispute through negotiation.

**12.2 Mediation.** If senior-executive negotiations are unsuccessful within the thirty (30) day period, either Party may initiate non-binding mediation administered by the ADR Institute of Canada under its applicable mediation rules. Mediation shall take place in Toronto, Ontario, Canada. The costs of mediation shall be shared equally between the Parties.

**12.3 Arbitration.** If mediation does not resolve the dispute within sixty (60) days of its commencement (or such longer period as the Parties agree in writing), either Party may submit the matter to final and binding arbitration administered by the ADR Institute of Canada under its National Arbitration Rules (Commercial), before a single arbitrator with expertise in technology and healthcare law, conducted in Toronto, Ontario, Canada. The language of arbitration shall be English. The arbitrator's award shall be final and binding and may be entered as a judgment in any court of competent jurisdiction. The arbitrator shall have no authority to award punitive or exemplary damages except as permitted by statute.

**12.4 Governing Law.** This Agreement and all disputes arising out of or in connection with it (whether contractual or non-contractual) are governed by, and shall be construed in accordance with, the laws of the Province of Ontario and the federal laws of Canada applicable therein, without regard to conflict of laws principles. For Health Data handled under this Ontario form, PHIPA and other applicable Ontario and Canadian privacy laws govern Provider's obligations as set out in Exhibit B.

**12.5 Jurisdiction.** To the extent any dispute is not subject to arbitration under this Article 12, the Parties irrevocably attorn to and submit to the exclusive jurisdiction of the Ontario Superior Court of Justice, sitting in Toronto, Ontario, Canada, and any appellate courts therefrom. Each Party irrevocably waives any objection to the laying of venue in, and any objection to the exercise of jurisdiction by, such courts, including any objection on the grounds of forum non conveniens or inconvenient forum.

**12.6 Injunctive Relief.** Notwithstanding Sections 12.1 through 12.3, either Party may seek interim or permanent injunctive or other equitable relief from the Ontario Superior Court of Justice, sitting in Toronto, Ontario, Canada, and any appellate courts therefrom, to prevent or restrain an actual or threatened breach of Articles 6, 7, or 11, without the requirement to post bond or other security and without the necessity of proving actual damages. Such an application does not waive the right to arbitrate the underlying dispute.

**12.7 Regulatory Compliance.** Both Parties shall comply with all applicable federal, provincial, state, and local laws governing privacy, data protection, and health information in the performance of their obligations under this Agreement.

---

## ARTICLE 13 — GENERAL PROVISIONS

**13.1 Entire Agreement.** This Agreement, together with all Order Forms, DPAs, exhibits, and schedules attached hereto, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior and contemporaneous agreements, proposals, negotiations, representations, and understandings, whether written or oral, relating to such subject matter.

**13.2 Amendments.** Provider may update the terms of this Agreement on thirty (30) days' prior written notice to Client. Continued use of the Services following the effective date of any such update constitutes Client's acceptance of the updated terms. Notwithstanding the foregoing, any material amendment to Article 7 (Data Protection) or the applicable DPA requires Client's prior written consent.

**13.3 Severability.** If any provision of this Agreement is found by a court or arbitrator of competent jurisdiction to be invalid, illegal, or unenforceable, such provision shall be modified to the minimum extent necessary to make it valid and enforceable, and the remaining provisions shall continue in full force and effect.

**13.4 Assignment.** Neither Party may assign or transfer this Agreement or any rights or obligations hereunder without the prior written consent of the other Party, which shall not be unreasonably withheld. Notwithstanding the foregoing, Provider may assign this Agreement without Client's consent in connection with a merger, acquisition, reorganization, or sale of all or substantially all of Provider's assets or business, provided that the assignee agrees in writing to be bound by the terms of this Agreement.

**13.5 Force Majeure.** Neither Party shall be liable for any delay or failure to perform its obligations under this Agreement (except for payment obligations and obligations relating to the security of Health Data) to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, pandemics, war, terrorism, civil unrest, government actions, internet outages, or failures of third-party infrastructure. The affected Party shall give prompt written notice and use commercially reasonable efforts to mitigate the impact. If such circumstances persist for more than sixty (60) consecutive days, either Party may terminate this Agreement on written notice without further liability.

**13.6 Notices.** All notices required or permitted under this Agreement shall be in writing and delivered: (a) by hand, effective upon receipt; (b) by registered mail, return receipt requested, effective three (3) business days after posting; (c) by nationally recognized overnight courier, effective the next business day; or (d) by email with confirmation of receipt (by reply email or read receipt), effective upon confirmed receipt. Notices shall be addressed to Provider at the address set out in the preamble, and to Client at the address or email on file with Provider.

**13.7 Waiver.** No waiver of any right or obligation under this Agreement shall be effective unless made in writing and signed by the waiving Party. No failure or delay by a Party in exercising any right shall operate as a waiver thereof, and no single or partial exercise of any right shall preclude any other or further exercise of that or any other right.

**13.8 Independent Contractors.** The Parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture, franchise, agency, employment relationship, or fiduciary duty between the Parties. Neither Party has authority to bind the other or to incur obligations on the other's behalf.

**13.9 No Third-Party Beneficiaries.** This Agreement is for the sole benefit of the Parties and their respective permitted successors and assigns. Nothing in this Agreement, express or implied, confers any right, remedy, or benefit upon any other person or entity.

**13.10 Electronic Acceptance.** By checking the "I agree to the Terms of Service" checkbox during checkout or by using the Services, Client acknowledges having read, understood, and agreed to be legally bound by all terms and conditions of this Agreement, including all applicable DPAs. This electronic acceptance constitutes a legally binding signature under Canada's PIPEDA and applicable provincial electronic commerce legislation, and the U.S. Electronic Signatures in Global and National Commerce Act (E-SIGN) and Uniform Electronic Transactions Act (UETA), as applicable.

**13.11 Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed an original. Electronic signatures shall be valid and binding to the same extent as original signatures.

**13.12 Publicity.** Neither Party shall issue press releases, public announcements, or other public statements regarding this Agreement or the business relationship between the Parties without the other Party's prior written consent, except as required by applicable law or regulatory authority.

**13.13 Recording and Monitoring.** Calls and interactions handled by the AI System may be recorded for quality assurance, training, and compliance purposes. Client is solely responsible for providing all notices to, and obtaining all consents from, patients and callers required under applicable recording consent and wiretapping laws, including any two-party or all-party consent requirements in Client's jurisdiction.

**13.14 No Medical Advice.** The AI System is an administrative tool only. It does not provide medical advice, diagnosis, or treatment, and is not a substitute for professional medical judgment. Client is solely responsible for all clinical decisions made in connection with the Services.

**13.15 Construction.** This Agreement shall be construed fairly as to both Parties, without regard to which Party drafted any particular provision. The word "including" means "including, without limitation." Headings are for convenience only and shall not affect interpretation.

**13.16 Compliance with Laws.** Each Party shall comply with all applicable federal, provincial, state, and local laws and regulations in the performance of its obligations under this Agreement, including all applicable privacy, data protection, and health information laws.

**13.17 Order of Precedence.** In the event of any conflict among the contractual documents, the following order of precedence shall apply: (a) the applicable DPA or BAA, solely with respect to privacy, security, and health information obligations; (b) the applicable Order Form or Service Order; (c) this Agreement; (d) Exhibit A; and (e) any other exhibit or schedule, unless such exhibit or schedule expressly states a different order of precedence.

**13.18 Third-Party Services.** Certain features of the Services depend on Third-Party Components, including communications providers, EHR/PMS vendors, calendar platforms, and payment processors such as Stripe. Client's use of Third-Party Components may be subject to separate third-party terms, privacy notices, availability limits, fees, reserves, fraud controls, or technical constraints. Provider is not responsible for the acts or omissions of such third parties except as expressly stated in this Agreement.

**13.19 No Reliance on Future Features.** Client acknowledges that it has not entered into this Agreement in reliance on any future functionality, product roadmap item, feature enhancement, or service availability that is not expressly set out in the applicable Order Form.

**13.20 Support Requests.** Client may submit support or assistance requests through the support contact, support email address, ticketing portal, or other support channel designated by Provider in the applicable Service Order, onboarding materials, or Documentation. Provider shall use commercially reasonable efforts to respond in accordance with any applicable Service Level Agreement or support commitments expressly stated in the applicable Service Order. Unless expressly agreed in writing, Provider is not obligated to provide custom development, implementation consulting, or support outside stated support scope or support hours as part of the base Fees.

---

## ARTICLE 14 — INSURANCE

**14.1 Coverage.** Provider shall maintain, at its own expense throughout the Term, commercially reasonable insurance appropriate to its operations and the Services provided, including: (a) commercial general liability insurance; (b) professional liability / errors and omissions insurance; and (c) cyber liability and data breach insurance. Provider shall furnish certificates of insurance to Client upon Client's reasonable written request.

---

**ELECTRONIC ACCEPTANCE**

By checking the "I agree to the Terms of Service" checkbox on the payment or onboarding page, Client acknowledges that it has read, understood, and agrees to be legally bound by all terms and conditions of this Agreement, including the applicable Data Protection Addendum.

**Provider:** 2771764 Ontario Inc. c.o.b. as Ample AI

**Client:** Accepted electronically at checkout

**EXHIBIT A — SERVICE LEVEL AGREEMENT**

Provider shall use commercially reasonable efforts to maintain the following service levels:

<b>Metric</b>	<b>Target</b>	<b>Remedy</b>
Uptime	99.5% monthly	Service credit of 5% of monthly fee per 0.5% below target
Support Response	24 hours (business days)	Escalation to senior support team
Critical Incident Resolution	72 hours	Root cause analysis provided in writing
Data Backup	Daily encrypted backups	Restoration within 24 hours

Service credits are Client's sole and exclusive remedy for Provider's failure to meet uptime targets and shall not exceed twenty-five percent (25%) of the applicable monthly fee in any calendar month. Service credits do not apply to downtime caused by Client's actions, third-party platform failures, or scheduled maintenance of which Client received advance notice.

## **EXHIBIT B — ONTARIO PHIPA SERVICE PROVIDER PRIVACY AGREEMENT**

*This Exhibit B ("Ontario Privacy Agreement") is entered into as of the Effective Date and forms part of the Master Services Agreement between the Parties (the "Agreement"). In the event of any conflict between this Exhibit B and the body of the Agreement with respect to the collection, use, disclosure, or protection of Personal Health Information, this Exhibit B shall control.*

**Health Information Custodian ("Custodian"):** The Client identified in the Agreement.

**Agent:** 2771764 Ontario Inc. carrying on business as Ample AI ("Provider").

**WHEREAS**, Custodian is a health information custodian within the meaning of Ontario's Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, as amended ("PHIPA"), responsible for Personal Health Information in its custody or control;

**WHEREAS**, Agent performs services for Custodian that require Agent to collect, use, disclose, retain, or handle Personal Health Information on Custodian's behalf, constituting Agent as an "agent" within the meaning of PHIPA, s. 17;

**NOW, THEREFORE**, the Parties agree as follows:

---

### **B-1. DEFINITIONS**

Capitalized terms used but not defined in this Exhibit B have the meanings given in the Agreement. The following additional definitions apply:

**B-1.1** "Agent" has the meaning given in PHIPA, s. 17, and refers to Provider in the context of this Exhibit.

**B-1.2** "Custodian" means the health information custodian (Client) identified above.

**B-1.3** "IPC" means the Information and Privacy Commissioner of Ontario.

**B-1.4** "Personal Health Information" or "PHI" means personal health information as defined in PHIPA, s. 4, including information about the physical or mental health of an identifiable individual, health care services provided, health card numbers, or the identity of a substitute decision-maker.

**B-1.5** "PHIPA" means Ontario's Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, and its regulations, as amended from time to time.

**B-1.6** "Privacy Breach" means any unauthorized collection, use, or disclosure of PHI, or any action or circumstance that has occurred or may occur that could result in unauthorized access to, or unauthorized collection, use, modification, or disclosure of PHI, as described in PHIPA, s. 12.

**B-1.7** "Purpose" means the purposes for which Agent collects, uses, or discloses PHI on behalf of Custodian, as described in the Agreement and the applicable Service Order.

**B-1.8** "Sub-Agent" means any subcontractor, agent, or third party engaged by Agent that handles PHI on Agent's behalf.

## **B-2. SCOPE AND AUTHORIZATION**

**B-2.1 Authorization.** Agent is authorized by Custodian to collect, use, disclose, retain, and handle PHI solely for the Purpose and in accordance with the conditions and restrictions set out in this Exhibit, the Agreement, and any lawful written instructions from Custodian. Nothing in this Exhibit or the Agreement causes Agent to become a health information custodian under PHIPA, and Custodian retains responsibility for its obligations as a health information custodian.

**B-2.2 No Independent Use.** Agent shall not use PHI for any purpose other than the Purpose, including its own management, marketing, product development, AI model training (except for the direct benefit of Custodian with express prior written consent and proper de-identification), or any commercial purpose unrelated to the Services.

**B-2.3 Minimum Necessary.** Agent shall collect, use, and disclose only the minimum amount of PHI necessary to accomplish the Purpose, consistent with PHIPA's data minimization principles.

**B-2.4 Compliance with Instructions.** Agent shall promptly comply with Custodian's lawful written instructions regarding the handling of PHI and shall notify Custodian within five (5) business days in writing if it is unable to comply with any instruction or condition.

---

## **B-3. PERMITTED USES AND DISCLOSURES**

**B-3.1 Permitted.** Agent may collect, use, or disclose PHI only: (a) as directed by Custodian for the Purpose; (b) to a person to whom Custodian may disclose the information under PHIPA; (c) as required by applicable law or court order; (d) where Agent reasonably believes disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to a person, as permitted by PHIPA, s. 40; or (e) to another agent of Custodian, as directed by Custodian.

**B-3.2 Prohibited.** Agent shall not: (a) disclose PHI to any Sub-Agent except in accordance with Section B-6; (b) use or disclose PHI for its own purposes unrelated to the Services; (c) sell, trade, or otherwise commercialize PHI; (d) use PHI to train any AI model without Custodian's express prior written consent and proper de-identification; or (e) access PHI subject to a PHIPA "lockbox" designation under PHIPA, s. 52(1)(b) without the express prior consent of the individual to whom it relates.

---

## **B-4. PRIVACY AND SECURITY OBLIGATIONS**

**B-4.1 Safeguards.** Agent shall implement and maintain the minimum security baseline set out in Section 7.4 of the Agreement and such additional safeguards as are appropriate to the sensitivity of the PHI, including: (a) encryption of PHI at rest (AES-256 or equivalent) and in transit (TLS 1.2 or higher); (b) role-based access controls limiting access to personnel who require access to perform the Services; (c) multi-factor authentication for all systems processing PHI; (d) comprehensive audit logging of all access, use, and modification of PHI; (e) regular vulnerability assessments and documented incident response procedures; and (f) documented privacy training for all personnel with access to PHI.

**B-4.2 Conditions and Restrictions.** Agent shall comply with all conditions and restrictions imposed by Custodian with respect to the use or disclosure of PHI and shall notify Custodian immediately in writing if it becomes unable to comply with any condition or restriction.

**B-4.3 Accuracy.** Agent shall promptly notify Custodian in writing of any PHI in its custody or control that Agent has reason to believe is inaccurate, incomplete, or outdated, so that Custodian may take corrective action under PHIPA, s. 55.

**B-4.4 Record-Keeping.** Agent shall maintain records of all uses and disclosures of PHI sufficient to enable Custodian to respond to individual access and correction requests and to provide an accounting of disclosures as required by PHIPA.

---

## **B-5. PRIVACY BREACH NOTIFICATION AND RESPONSE**

**B-5.1 Notification Obligation.** Agent shall notify Custodian of any Privacy Breach involving PHI at the first reasonable opportunity and, in any event, without undue delay after Agent becomes aware of the breach. Agent shall provide an initial notice promptly even if full details are not yet available and shall supplement that notice as additional information becomes available.

**B-5.2 Content of Notification.** The notification shall include, to the extent known at the time and supplemented as additional information becomes available: (a) the date(s) and circumstances of the Privacy Breach; (b) the categories and approximate volume of PHI involved; (c) the number of individuals affected; (d) the identity of any unauthorized persons involved, to the extent known; (e) the immediate steps taken to contain and mitigate the Privacy Breach; (f) steps taken or proposed to notify affected individuals; (g) whether notification to the IPC has been or will be made; and (h) any other information Custodian requires to fulfill its notification obligations under PHIPA.

**B-5.3 Cooperation.** Agent shall cooperate fully with Custodian in any investigation, remediation, or regulatory notification relating to a Privacy Breach, including providing access to relevant records, systems, and personnel. Agent shall not communicate with affected individuals or the IPC regarding a Privacy Breach without Custodian's prior written authorization.

**B-5.4 Costs.** Agent shall bear the reasonable direct costs of Privacy Breach response (including forensic investigation and notifications) arising primarily from Agent's acts or omissions, in accordance with the indemnification provisions in Article 10 of the Agreement.

**B-5.5 Assistance with Custodian Reporting.** Agent shall provide reasonable cooperation and records requested by Custodian to enable Custodian to satisfy PHIPA breach notification, investigation, and annual statistical reporting obligations applicable to Custodian.

---

## **B-6. SUB-AGENTS**

**B-6.1 Authorization.** Custodian provides a general authorization for Agent to engage Sub-Agents to handle PHI on Agent's behalf, provided that Agent: (a) uses only Sub-Agents with a legitimate need to perform part of the Services; (b) imposes written obligations on each Sub-Agent that are no less protective than those in this Exhibit with respect to the PHI involved; (c) remains fully responsible for the acts and omissions of its Sub-Agents; and (d) provides advance notice of any material new Sub-Agent where required by the Agreement or applicable law.

---

**B-6.2 Written Agreement.** Agent shall require each approved Sub-Agent to execute a written agreement imposing PHIPA-compliant obligations substantially equivalent to those in this Exhibit, including obligations regarding security safeguards, breach notification, return or destruction of PHI, and restrictions on use and disclosure.

**B-6.3 Accountability.** Agent remains fully responsible and accountable to Custodian for all acts and omissions of its Sub-Agents. Agent shall maintain a current list of Sub-Agents handling PHI and shall make such list available to Custodian on written request.

---

## **B-7. INDIVIDUAL ACCESS RIGHTS**

**B-7.1 Access and Correction.** Agent shall, on Custodian's written request and within the timeframe specified by Custodian (no later than the timeframe required by PHIPA): (a) make available PHI in its custody or control to enable Custodian to respond to individual access requests under PHIPA, s. 52; (b) cooperate with Custodian to implement corrections to PHI in response to correction requests under PHIPA, s. 55; and (c) provide a record of disclosures of PHI to support Custodian's obligations under PHIPA.

**B-7.2 Lockbox.** Agent shall not access, use, or disclose PHI designated as subject to PHIPA's "lockbox" provisions (PHIPA, s. 52(1)(b)) without the express prior written consent of the individual to whom it relates.

---

## **B-8. RETURN AND DESTRUCTION OF PHI**

**B-8.1 Obligation.** On termination of the Agreement, or on written request by Custodian, Agent shall, at Custodian's election: (a) return all PHI (and all copies) to Custodian in a format reasonably specified by Custodian; or (b) securely destroy all PHI, including all copies in backup, disaster recovery, and archived systems, using methods rendering the PHI permanently irretrievable (NIST SP 800-88 or equivalent).

**B-8.2 Timeline.** Agent shall complete return or destruction within sixty (60) days of the effective date of termination or receipt of Custodian's written request.

**B-8.3 Certification.** Agent shall certify completion in writing within five (5) business days, identifying: (a) the date(s) of destruction; (b) the categories and volume of PHI; (c) the destruction method used; and (d) the name and title of the individual overseeing destruction.

**B-8.4 Infeasibility.** Where immediate destruction of certain PHI is technically infeasible (e.g., integration into backup systems that cannot selectively purge): (a) Agent shall notify Custodian in writing, identifying the PHI and the reason; (b) Agent shall continue to apply all protections of this Exhibit; (c) Agent shall limit further use to the minimum necessary; and (d) Agent shall destroy such PHI at the earliest feasible opportunity with immediate written certification.

---

## **B-9. LEGAL PROCESS AND REGULATORY ACCESS**

**B-9.1 Legal Process.** If Agent receives a subpoena, court order, access request, or other legal process requiring disclosure of PHI: (a) Agent shall notify Custodian in writing within forty-eight (48) hours of receipt to the extent permitted by law; (b) Agent shall cooperate with Custodian in seeking a protective order; (c) Agent shall disclose only the minimum PHI legally required; and (d) Agent shall not disclose PHI until Custodian has had a reasonable opportunity to respond, unless legally compelled sooner.

**B-9.2 IPC Access.** Agent shall make its internal practices, books, and records relating to the handling of PHI available to the IPC for any investigation, audit, or review under PHIPA upon reasonable notice.

**B-9.3 Regulatory Cooperation.** Agent shall cooperate with Custodian in responding to any complaint, investigation, or order from the IPC or other regulatory authority with jurisdiction over the handling of PHI.

---

## **B-10. AUDIT AND ACCOUNTABILITY**

**B-10.1 Records.** Agent shall maintain records sufficient to demonstrate compliance with this Exhibit for a minimum of seven (7) years following termination of the Agreement, or such longer period as required by PHIPA.

**B-10.2 Audit Rights.** On not less than thirty (30) days' prior written notice, Custodian may commission an independent audit of Agent's compliance with this Exhibit, no more than once per calendar year (or more frequently following a Privacy Breach). Agent may satisfy this requirement by providing a current SOC 2 Type II, HITRUST, or ISO 27001 certification.

**B-10.3 Privacy Officer.** Agent shall designate a qualified Privacy Officer responsible for overseeing compliance with PHIPA and this Exhibit. Agent shall provide the Privacy Officer's name and contact information to Custodian upon request.

**Custodian (Client):** Accepted electronically as part of the Master Services Agreement.

**Agent (Provider):** 2771764 Ontario Inc. c.o.b. as Ample AI