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: 7610262 Canada Inc., carrying on business as Ample AI, with its principal place of business at 100 King Street West, Suite 5600, Toronto, ON M5X 1C9 ("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, including inbound referral intake and administrative priority 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 disclosing to patients that they may be interacting with an AI system, in compliance with all applicable laws and regulations in Client's jurisdiction.

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.

2.8 Administrative Routing — Scope of the Term 'Triage.' Where the Services include functionality described as 'triage,' 'patient triage,' or 'priority routing,' these terms refer exclusively to administrative routing: the process of gathering information from callers or patients and directing them to an appropriate next step (such as scheduling an appointment, transferring to a specific provider, or flagging a matter for staff follow-up) in accordance with Client's pre-approved protocols. 'Triage' as used in this Agreement does not mean, and shall not be construed to include, clinical triage performed by or under the supervision of a licensed health professional pursuant to any formal clinical triage methodology, including the Canadian Triage and Acuity Scale, the Emergency Severity Index, or any similar system. Provider is not a licensed health professional and does not perform clinical assessments or determinations of medical urgency.

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 all patient consents, authorizations, and opt-ins required under applicable law, including consents for automated communications, AI interactions, and the collection and use of Health Data. Client is solely responsible for establishing lawful consent processes for patients who are minors, lack capacity, or require a substitute decision-maker or legal guardian, and for configuring the AI System to route such callers to appropriate human staff rather than proceeding through automated workflows.

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, 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, or non-compliant communication.

3.10 Clinical Protocol Ownership and Written Sign-Off. All triage criteria, urgency classifications, escalation rules, appointment booking logic, routing rules, patient scripts, fallback workflows, and any other clinical or operational decision pathways implemented through the Services are defined, owned, and controlled exclusively by Client. Provider's role is solely to implement Client's approved instructions through the AI System — Provider does not independently determine clinical appropriateness, urgency, or patient care pathways. Client shall: (a) provide all such protocols, rules, and decision criteria to Provider in writing prior to deployment; (b) review and provide written approval — including by email or electronic confirmation — of all configurations and workflows before production use and following any material change; and (c) promptly notify Provider of any error, unsafe response, or change in clinical protocol requiring reconfiguration. Client's written approval of any configuration constitutes Client's representation that the configuration is clinically appropriate, lawful, and fit for the intended purpose. Provider has no responsibility or liability for any outcome — including misrouting, delayed care, inappropriate escalation, patient harm, or death — arising from the operation of any protocol or decision pathway that was defined, approved, or required by Client.

3.11 Referral Intake and Priority Classification. Where Client uses the Services to receive and process inbound referrals from other healthcare providers or their staff: (a) Client is solely responsible for defining and maintaining the criteria by which referrals are classified by priority (routine, semi-urgent, urgent, or otherwise) and routed within Client's practice; (b) all priority classifications, routing rules, booking windows, and acknowledgment timelines applied by the AI System to inbound referrals are defined exclusively by Client's pre-approved protocols; (c) Client shall maintain a staffed review process to action referral requests within the timeframes required by Client's clinical standards, College obligations, and applicable law; and (d) Provider shall have no liability for any adverse outcome — including patient harm, clinical deterioration, or delayed specialist care — arising from a referral priority classification or routing decision made in accordance with Client's approved protocols.

3.12 Prescription and Controlled Substance Routing. The Services may route prescription refill requests and medication-related inquiries in accordance with Client's defined protocols. Provider does not verify the clinical appropriateness of any prescription request, check for drug interactions, access prescribing systems, confirm patient eligibility for controlled substances, or perform any function reserved to licensed prescribers, pharmacists, or regulated health professionals under applicable law. Client is solely responsible for ensuring that any prescription or refill routing workflow configured through the Services complies with all applicable regulatory requirements, including the U.S. Controlled Substances Act and DEA requirements (for U.S. clients), provincial regulatory college standards (for Canadian clients), and any applicable drug scheduling or controlled substance legislation. Provider shall have no liability for any adverse outcome arising from prescription routing decisions made in accordance with Client's approved protocols.

3.13 Vulnerable Caller Handling. Client is solely responsible for defining and maintaining escalation rules for callers who may be in crisis, distress, or a vulnerable state — including callers expressing suicidal ideation, self-harm intentions, domestic violence situations, or severe medical distress. Client shall configure the AI System to immediately escalate such callers to a human staff member or emergency service in accordance with Client's approved protocols. Provider is not responsible for identifying, assessing, or intervening in vulnerable caller situations beyond executing the escalation logic Client has approved and deployed. Provider shall have no liability for any adverse outcome — including death, self-harm, or any failure to identify, escalate, or intervene — arising from the operation of any

vulnerable-caller escalation rule defined, approved, or required by Client, which is governed by Sections 3.10 and 9.8.

3.14 Call Recording Disclosure Configuration. Prior to enabling call recording in any jurisdiction, Client shall: (a) determine whether applicable federal, provincial, state, or local law requires notice to, or consent from, one or all parties to a call before the call may be recorded — including, in the United States, all-party or two-party consent requirements under state wiretapping statutes applicable to Client's jurisdiction(s) of operation; (b) provide Provider with a written, approved recording disclosure script that satisfies all such legal requirements, specifying the exact wording to be delivered by the AI System at the start of each recorded call, and the required caller response (if any) before recording begins; (c) specify in writing the fallback procedure to be applied if a caller declines recording — including whether the call should continue unrecorded, be transferred to a human agent, or be terminated; and (d) promptly notify Provider in writing of any change in applicable recording consent law that requires modification of the disclosure script. Provider shall implement Client's approved disclosure script verbatim within the call flow. Client represents and warrants that its approved script satisfies all applicable recording consent and wiretapping laws, and Client bears sole responsibility for the legal sufficiency of that script. Provider shall have no liability for any recording consent violation that arises from Provider's implementation of a disclosure script approved by Client, or from Client's failure to supply or update a required disclosure script.

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 Service Fee. A recurring monthly service fee as specified in the applicable Order Form (the "Monthly Service Fee"), due and payable thirty (30) days following the Effective Date and every thirty (30) days thereafter. Monthly Service 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.

4.2 Payment Authorization. Provider shall issue invoices for Monthly Service Fees no later than five (5) business days prior to each due date. Client shall maintain valid payment information on file and authorizes Provider to charge the applicable payment method on each due date for all fees owed under this Agreement.

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. Client shall reimburse Provider for all

reasonable collection costs, including reasonable attorneys' fees. Provider may suspend Services upon fifteen (15) days' prior written notice if any undisputed amount remains unpaid after its due date.

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 increase fees effective at the start of any renewal term on not less than sixty (60) days' prior written notice. Provider shall not increase fees during the Initial Term except as expressly specified in the Service Order, and any such Initial-Term increase shall not exceed five percent (5%) per annum.

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.

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, the Initial Term is typically twelve (12) months, renewing automatically for successive twelve (12) month periods unless either Party provides written notice of non-renewal at least sixty (60) days before the end of the then-current term. 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) accrued Monthly Service Fees remain due and payable; (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, either Party may terminate this Agreement on ninety (90) days' prior written notice; if Client terminates during the Initial Term, Client shall pay an early termination fee equal to the lesser of (i) the remaining Monthly Service Fees for the balance of the Initial Term or (ii) three (3) months of Monthly Service Fees at the then-current rate, unless otherwise specified in the Service Order; 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 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, Health Data, or any de-identified or aggregated derivative thereof to train, fine-tune, or improve any machine learning or artificial intelligence model without Client's express prior written consent. This restriction applies regardless of whether the intended purpose is described as related to the Services. 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 for Provider's internal analytics, service monitoring, and operational improvement (excluding model training or fine-tuning, which is governed exclusively by Section 6.5), 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) 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 Reference and Case Study Rights. Client hereby grants Provider a non-exclusive, royalty-free, perpetual license to: (a) identify Client by name, logo, and practice description as a customer of Provider in Provider's website, marketing materials, pitch decks, sales presentations, investor materials, press, and

other promotional content; (b) develop and publish case studies, success stories, and testimonials based on Client's experience with the Services, including operational and business metrics (such as call volume reductions, booking rates, and patient satisfaction scores), subject to Client's prior review of specific metrics proposed for publication, such review not to be unreasonably delayed or withheld; and (c) reference Client by name or logo in speaking engagements, conferences, and media. Provider shall not publish case study content containing patient-identifiable information or information Client reasonably designates as confidential. Client may withdraw consent to future use on sixty (60) days' written notice; materials published prior to such withdrawal may remain in circulation. Neither Party shall use the other's trademarks in a manner that implies endorsement beyond what is expressly permitted in this Section 6.7.

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 is governed by the Data Protection Addendum ("DPA") attached hereto and incorporated by reference. The applicable DPA is determined by Client's primary jurisdiction of operation as follows:

(a) Ontario, Canada: Exhibit B — Ontario PHIPA Service Provider Privacy Agreement;

(b) British Columbia, Canada: Exhibit C — BC PIPA Service Provider Privacy Agreement;

(c) All other Canadian provinces and territories (excluding Quebec): Exhibit D — Canada (Other Provinces) PIPEDA Service Provider Privacy Agreement; and

(d) United States of America: Exhibit E — HIPAA Business Associate Agreement.

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.

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, 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.

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 and authorizations required by applicable law prior to providing Health Data to Provider; (c) all information provided by Client to Provider is, to Client's knowledge, accurate, complete, and lawfully provided; and (d) Client shall use the Services solely for the Permitted Purpose.

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, or other issues caused by Third-Party Components, telecommunications carriers, internet service providers, or Client systems, except to the extent caused by Provider's breach of this Agreement.

9.8 CLINICAL PROTOCOL LIABILITY EXCLUSION. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, PROVIDER SHALL HAVE NO LIABILITY WHATSOEVER — INCLUDING FOR PERSONAL INJURY, DEATH, DELAYED CARE, MISROUTING, OR ANY ADVERSE CLINICAL OUTCOME — ARISING FROM THE OPERATION OF ANY TRIAGE LOGIC, URGENCY CRITERIA, ESCALATION RULE, ROUTING RULE, SCRIPT, BOOKING CRITERIA, OR OTHER CLINICAL OR OPERATIONAL DECISION PATHWAY THAT WAS DEFINED, APPROVED, OR REQUIRED BY CLIENT PURSUANT TO SECTION 3.10. PROVIDER IS NOT A HEALTHCARE PROVIDER, DOES NOT EXERCISE CLINICAL JUDGMENT, AND HAS NO INDEPENDENT OBLIGATION TO ASSESS THE SAFETY OR APPROPRIATENESS OF CLIENT'S PROTOCOLS. ALL LIABILITY FOR CLINICAL OUTCOMES, TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, RESTS WITH CLIENT AS THE LICENSED OPERATOR OF ITS HEALTHCARE PRACTICE AND THE SOLE AUTHOR OF ITS CLINICAL DECISION PATHWAYS.

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; (j) Client's use of the Services for emergency, diagnostic, treatment, or other high-risk purposes not expressly authorized under this Agreement; or (k) any claim by a patient, regulator, insurer, or third party arising from patient harm, injury, death, delayed care, misrouting, or adverse clinical outcome attributable to any triage logic, urgency criteria, escalation rule, routing rule, script, or clinical decision pathway defined, approved, or required by Client pursuant to Section 3.10.

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 U.S. clients, U.S. federal law (including HIPAA and HITECH) and applicable U.S. state privacy law govern Provider's obligations with respect to Health Data as set out in Exhibit E. For BC clients, BC PIPA governs Provider's obligations with respect to Health Data as set out in Exhibit C. For clients in other Canadian provinces, PIPEDA and applicable provincial health information law govern Provider's obligations with respect to Health Data as set out in Exhibit D.

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 any court of competent jurisdiction 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 non-material 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. Any material amendment — including any change to fees, service scope, liability limits, data protection obligations (including Article 7 and the applicable DPA), or indemnification — requires Client's prior written consent before taking effect. A change is "material" if it would reasonably be expected to affect Client's rights, obligations, or risk exposure under this Agreement.

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 or public statements regarding this Agreement or the business relationship between the Parties without the other Party's prior written consent, except: (a) Provider may identify Client as a customer and publish case studies and reference materials in accordance with Section 6.7 without further consent; and (b) either Party may make statements 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, compliance, and service improvement purposes. Provider will configure call recording disclosures in the AI System in accordance with Client's written instructions under Section 3.14. Client is solely responsible for the legal sufficiency of all recording disclosures and consents, including compliance with any two-party or all-party consent requirements in Client's jurisdiction(s) of operation. Provider has no liability for recording consent violations arising from Client's approved disclosure script or from Client's failure to provide or update a disclosure script as required under Section 3.14.

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. Client's use of Third-Party Components may be subject to separate third-party terms, privacy notices, availability limits, fees, 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.

ARTICLE 14 — INSURANCE

14.1 Provider 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.

14.2 Client Coverage. Client shall maintain throughout the Term, at its own expense: (a) professional liability (medical malpractice) insurance in amounts appropriate to Client's practice type, size, and jurisdiction; and (b) commercial general liability insurance. Client shall furnish evidence of such coverage to Provider upon reasonable written request. Provider may suspend Services on thirty (30) days' written notice if Client fails to maintain required coverage and does not provide satisfactory evidence of coverage within that period.

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: 7610262 Canada 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:

Metric	Target	Remedy
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 E — HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA" or "Exhibit E") is entered into as of the Effective Date and is incorporated into and made a part of the Master Services Agreement between the Parties (the "Agreement"). In the event of any conflict between this Exhibit E and the body of the Agreement with respect to HIPAA obligations or the handling of Protected Health Information, this Exhibit E shall control.

Covered Entity ("CE"): The healthcare provider or entity identified as Client in the Agreement.

Business Associate ("BA"): 7610262 Canada Inc. carrying on business as Ample AI.

WHEREAS, CE is a Covered Entity as defined under the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the regulations at 45 CFR Parts 160 and 164 (collectively, "HIPAA");

WHEREAS, BA provides services to CE that require BA to create, receive, maintain, or transmit Protected Health Information on behalf of CE, thereby qualifying BA as a Business Associate under HIPAA;

WHEREAS, 45 CFR § 164.308(b) and 45 CFR § 164.502(e) require CE and BA to enter into a written BAA meeting the requirements of the HIPAA Rules; and

NOW, THEREFORE, the Parties agree as follows:

E-1. DEFINITIONS

The following terms have the meanings set out below. Terms used but not defined in this Exhibit E have the meanings given in the HIPAA Rules or the Agreement.

E-1.1 "Breach" means the acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI, as defined at 45 CFR § 164.402.

E-1.2 "Business Associate" or "BA" means 7610262 Canada Inc. c.o.b. as Ample AI, as defined at 45 CFR § 160.103.

E-1.3 "Covered Entity" or "CE" means the Client identified in the Agreement, as defined at 45 CFR § 160.103.

E-1.4 "Designated Record Set" has the meaning set out at 45 CFR § 164.501.

E-1.5 "Electronic PHI" or "ePHI" means PHI that is created, received, maintained, or transmitted in electronic form, as defined at 45 CFR § 160.103.

E-1.6 "HIPAA Rules" means, collectively, the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule promulgated under HIPAA and HITECH at 45 CFR Parts 160 and 164.

E-1.7 "Individual" means the person who is the subject of PHI, as defined at 45 CFR § 160.103.

E-1.8 "Privacy Rule" means the HIPAA Privacy Regulations at 45 CFR Part 164, Subpart E.

E-1.9 "Protected Health Information" or "PHI" means individually identifiable health information transmitted or maintained in any form or medium, as defined at 45 CFR § 160.103, limited to the PHI BA creates, receives, maintains, or transmits on behalf of CE.

E-1.10 "Required by Law" means a mandate contained in law that compels disclosure and that is enforceable in a court of law, as defined at 45 CFR § 164.103.

E-1.11 "Secretary" means the Secretary of the U.S. Department of Health and Human Services ("HHS"), or the Secretary's designee.

E-1.12 "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system, as defined at 45 CFR § 164.304.

E-1.13 "Security Rule" means the HIPAA Security Regulations at 45 CFR Part 164, Subparts A and C.

E-1.14 "Subcontractor" means a person to whom BA delegates a function, activity, or service, other than in the capacity of a workforce member, as defined at 45 CFR § 160.103.

E-1.15 "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable through a technology or methodology specified by the Secretary, as defined at 45 CFR § 164.402.

E-2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

E-2.1 Permitted Uses and Disclosures. BA shall not use or disclose PHI other than as permitted or required by this BAA or as Required by Law. BA may: (a) use and disclose PHI as necessary to perform the Services, including without limitation: handling inbound and outbound voice calls involving PHI; recording and storing call audio and voicemails; generating, storing, and indexing call transcripts; transmitting SMS, MMS, and similar electronic communications to or on behalf of CE; writing appointment records, intake data, and patient-record updates to CE's practice management system or electronic health record; and processing call content and related data through artificial intelligence, speech-to-text, text-to-speech, and large language model subprocessors engaged in accordance with §E-2.5; (b) use PHI for BA's proper management and administration, provided that any disclosure is Required by Law or BA obtains reasonable written assurances of confidentiality from the recipient; (c) use PHI to provide Data Aggregation services relating to CE's healthcare operations, if expressly requested by CE; and (d) de-identify PHI in accordance with 45 CFR § 164.514(a)–(c) and thereafter use and disclose de-identified data for any lawful purpose, provided BA does not attempt to re-identify it.

E-2.2 Prohibited Uses and Disclosures. BA shall not: (a) use or disclose PHI in a manner that would violate the HIPAA Rules if done by CE; (b) use PHI for BA's own marketing without CE's express prior written authorization; (c) sell PHI other than in connection with a merger, acquisition, or sale of BA's business; (d) use PHI, or any de-identified or aggregated derivative of PHI, to train, fine-tune, or improve any machine learning or artificial intelligence model, without CE's express prior written consent — this restriction applies regardless of whether the intended use is described as related to the Services; or (e) disclose PHI to any Subcontractor except in accordance with Section E-2.5.

E-2.3 Safeguards. BA shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI as required by the Security Rule (45 CFR Part 164, Subpart C), including:

(a) Administrative safeguards under 45 CFR § 164.308, including security management processes, workforce security, access management, security awareness and training, and contingency planning;

(b) Physical safeguards under 45 CFR § 164.310, including facility access controls, workstation security, and device and media controls; and

(c) Technical safeguards under 45 CFR § 164.312, including access controls (unique user IDs, emergency access, automatic logoff, encryption and decryption), audit controls, integrity controls, and transmission security (TLS 1.2 or higher in transit; AES-256 or equivalent at rest).

E-2.4 Breach Notification. BA shall report to CE any Breach of Unsecured PHI as soon as reasonably practicable and no later than seventy-two (72) hours after BA discovers the Breach. BA shall apply the four-factor risk assessment under 45 CFR § 164.402 to determine whether an impermissible use or disclosure constitutes a Breach. The notification shall include, to the extent known at the time and supplemented as information becomes available: (a) the date of the Breach and the date of discovery; (b) the nature of the impermissible use or disclosure; (c) the types of Unsecured PHI involved; (d) the number of Individuals affected; (e) whether PHI was actually acquired or viewed; (f) the extent to which risk has been mitigated; (g) corrective actions taken or planned; and (h) a designated contact for CE's follow-up. BA shall cooperate with CE in satisfying CE's Breach notification obligations to Individuals, the Secretary, and applicable state agencies under HIPAA, HITECH, and applicable state law.

E-2.5 Subcontractors. BA shall ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on BA's behalf executes a written BAA imposing substantially the same restrictions, conditions, and requirements as this Exhibit E. BA shall maintain a current Subcontractor list and make it available to CE on written request. BA remains responsible for all acts and omissions of its Subcontractors.

E-2.6 Individual Rights. BA shall support CE's obligations with respect to Individual rights under the HIPAA Rules: (a) Access (45 CFR § 164.524): BA shall make PHI in a Designated Record Set available to CE within fifteen (15) business days of CE's written request; (b) Amendment (45 CFR § 164.526): BA shall make PHI in a Designated Record Set available for amendment and shall incorporate amendments as directed by CE; and (c) Accounting of Disclosures (45 CFR § 164.528): BA shall document all disclosures of PHI and make documentation available to CE, retaining such records for at least six (6) years.

E-2.7 Access by Secretary. BA shall make available its internal practices, books, and records relating to the use and disclosure of PHI to the Secretary for purposes of determining CE's or BA's compliance with the HIPAA Rules.

E-2.8 Security Incident Reporting. BA shall report to CE, in writing and without undue delay, any Security Incident of which BA becomes aware. For attempted but unsuccessful Security Incidents (such as pings, port scans, and failed log-in attempts that do not result in unauthorized access), BA shall provide a summary report to CE on a quarterly basis.

E-2.9 Minimum Necessary. BA shall make reasonable efforts to use, disclose, and request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request, in accordance with 45 CFR § 164.502(b) and § 164.514(d).

E-2.10 Mitigation. BA shall mitigate, to the extent practicable, any harmful effect that is known to BA of a use or disclosure of PHI in violation of this BAA, including taking prompt corrective action and cooperating with CE in remediation efforts.

E-2.11 Policies and Procedures. BA shall maintain written policies and procedures implementing the requirements of this BAA and the HIPAA Rules, and shall document all actions, activities, and

assessments required to be documented under the HIPAA Rules. BA shall retain such documentation for a minimum of six (6) years from the date of creation or the date it was last in effect, whichever is later.

E-2.12 42 CFR Part 2 and Other Enhanced Confidentiality Regimes. If CE is subject to 42 CFR Part 2 or any comparable law imposing confidentiality, segregation, consent, or redisclosure obligations materially beyond HIPAA, CE shall notify BA before transmitting such data to BA. The Parties shall cooperate in good faith to determine whether an additional addendum or technical control set is required. Unless expressly agreed in writing, BA does not represent that the Services are configured to satisfy 42 CFR Part 2 or similar heightened requirements.

E-3. WORKFORCE TRAINING AND SECURITY AWARENESS

E-3.1 HIPAA Privacy Training. BA shall provide training on HIPAA Privacy Rule requirements and BA's related policies and procedures to all workforce members who create, receive, maintain, or transmit PHI on behalf of BA. Training shall be provided at hiring, updated as material changes occur, and refreshed annually. BA shall document that training has been provided and maintained.

E-3.2 Security Awareness and Training. BA shall implement a security awareness and training program for all workforce members, including management, in accordance with 45 CFR § 164.308(a)(5), including security reminders, protection from malicious software, log-in monitoring, and password management. BA shall document training completion and related security measures.

E-3.3 Security Officers. BA shall designate a HIPAA Security Officer responsible for developing, implementing, and overseeing the security program required by the Security Rule, and shall designate a HIPAA Privacy Officer responsible for developing and implementing privacy policies and procedures. Contact information for both Officers shall be provided to CE upon request.

E-4. OBLIGATIONS OF COVERED ENTITY

E-4.1 Notice of Privacy Practices. CE shall notify BA of any restriction on uses or disclosures of PHI agreed to in CE's Notice of Privacy Practices, and of any changes to such restrictions, to the extent such restrictions affect BA's permitted uses and disclosures under this BAA.

E-4.2 Individual Permissions and Restrictions. CE shall notify BA of any restriction on the use or disclosure of PHI that CE has agreed to with an Individual under 45 CFR § 164.522, to the extent such restriction affects BA's activities.

E-4.3 Notification of Changes. CE shall notify BA of any changes in, or revocation of, authorization by an Individual that would affect BA's use or disclosure of PHI, to the extent such changes affect BA's activities.

E-4.4 No Impermissible Requests. CE shall not request BA to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by CE, except where expressly permitted by this BAA.

E-4.5 Accurate Information. CE shall provide BA with accurate and complete information about CE's covered entity status, any applicable restrictions, and any state-specific requirements that impose obligations on BA beyond those required by HIPAA.

E-5. PERMITTED USES BY BA FOR OWN MANAGEMENT

BA may use and disclose PHI for BA's own management and administration or to fulfill BA's legal responsibilities, provided that: (a) such uses or disclosures are necessary for BA's management and administration or to carry out BA's legal responsibilities; (b) the information is used in a manner that does not violate the HIPAA Rules if performed by CE; and (c) where BA discloses PHI for its management and administration, (i) the disclosure is Required by Law, or (ii) BA obtains reasonable written assurances from the recipient that the PHI will be held confidentially, used or disclosed only as Required by Law or for the purpose for which it was disclosed, and that the recipient will notify BA of any known or suspected Breach.

E-6. RETURN AND DESTRUCTION OF PHI

E-6.1 Obligation. On termination of the Agreement, BA shall, at CE's election: (a) return all PHI (including all copies) to CE in a format reasonably specified by CE; or (b) securely destroy all PHI, including all copies in backup and disaster recovery systems, using NIST SP 800-88 recommended methods or equivalent, rendering the PHI permanently irretrievable.

E-6.2 Timeline. BA shall complete return or destruction within sixty (60) days of the effective date of termination.

E-6.3 Certification. BA shall certify completion in writing within five (5) business days, including: (a) the date(s) of return or destruction; (b) the categories and volume of PHI; (c) the method of destruction; and (d) the name and title of the responsible individual.

E-6.4 Infeasibility. Where BA determines that immediate destruction of certain PHI is technically infeasible: (a) BA shall notify CE in writing identifying the specific PHI and the reason; (b) BA shall extend the protections of this BAA to such PHI; (c) BA shall limit further uses and disclosures to those purposes that make return or destruction infeasible; and (d) BA shall destroy the PHI at the earliest feasible opportunity with immediate written certification to CE.

E-6.5 Reporting to HHS. If CE determines that termination of this BAA is not feasible due to the nature of the services, CE shall report the violation to the Secretary in accordance with 45 CFR § 164.504(e)(1)(ii).

E-7. TERM AND TERMINATION

E-7.1 Term. This BAA is effective as of the Effective Date and shall remain in effect until the termination or expiration of the Agreement, unless earlier terminated as provided herein.

E-7.2 Termination for Cause. If either Party determines that the other has materially breached a material provision of this BAA: (a) the non-breaching Party shall provide written notice identifying the breach in reasonable detail; (b) the breaching Party shall have thirty (30) days to cure the breach; and (c) if the breach is not cured within such period, the non-breaching Party may terminate this BAA and the Agreement immediately on written notice. If cure is not possible, the non-breaching Party may terminate immediately upon written notice.

E-7.3 Termination by CE. CE may terminate this BAA and the Agreement immediately, without opportunity to cure, if CE reasonably determines that BA has engaged in a pattern of activity or practice constituting a material violation of this BAA that creates a significant ongoing risk to PHI or to CE's HIPAA compliance.

E-7.4 Survival. The following provisions survive termination of this BAA: Section E-6 (Return and Destruction); Section E-2.11 (Policies and Procedures, for documentation retention); Section E-8 (Amendment); Section E-9 (No Third-Party Beneficiaries); and Section E-10 (Miscellaneous), including the obligation to comply with the HIPAA Rules for any PHI that cannot immediately be returned or destroyed.

E-8. AMENDMENT

E-8.1 Automatic Amendment. This BAA shall automatically be amended, without further action by the Parties, to the extent necessary to comply with any amendment to HIPAA, HITECH, or the HIPAA Rules that modifies requirements applicable to business associate agreements, effective as of the compliance date of such amendment.

E-8.2 Negotiated Amendment. The Parties shall negotiate in good faith any additional amendments to this BAA required to ensure ongoing compliance with applicable law. Any such amendment shall be in writing and signed by authorized representatives of both Parties.

E-9. NO THIRD-PARTY BENEFICIARIES

Nothing in this BAA shall be construed to create any rights in or on behalf of any third party, including any Individual whose PHI is the subject of this BAA. This BAA is for the sole benefit of CE and BA and their respective permitted successors and assigns.

E-10. MISCELLANEOUS

E-10.1 Interpretation. This BAA shall be interpreted to comply with HIPAA and the HIPAA Rules. Any ambiguity shall be resolved to permit compliance with the HIPAA Rules.

E-10.2 Regulatory References. Any reference to a section of the Code of Federal Regulations or the HIPAA Rules means such section as in effect or as amended from time to time.

E-10.3 Relationship of Parties. This BAA does not create a partnership, joint venture, or agency relationship between the Parties.

E-10.4 State Privacy Laws. CE shall notify BA of any applicable state health privacy laws (including, without limitation, the California Confidentiality of Medical Information Act, Texas Health & Safety Code Chapter 181, and New York's SHIELD Act) that impose obligations on BA beyond HIPAA requirements. Both Parties shall cooperate in good faith to comply with applicable state requirements.

E-10.5 Entire Agreement as to PHI. This BAA, together with the privacy and security provisions of the Agreement, constitutes the entire agreement between the Parties with respect to the protection of PHI and supersedes all prior agreements relating to such subject matter.

E-10.6 Indemnification. BA shall defend, indemnify, and hold harmless CE and its directors, officers, employees, and agents from and against any Losses arising from: (a) BA's breach of this BAA; or (b) BA's violation of the HIPAA Rules or other applicable law relating to PHI, except to the extent caused by CE's negligence or wilful misconduct. This section supplements, and does not limit, the indemnification obligations in Article 10 of the Agreement.

Covered Entity (CE / Client): Accepted electronically as part of the Master Services Agreement.

Business Associate (BA / Provider): 7610262 Canada Inc. c.o.b. as Ample AI