**Schedule “I”**

**Mandatory Provisions Schedule**

The following provisions shall be inserted by the Vendor in, and shall be deemed to form part of, every Purchasing Document between Vendor and a Buyer for AI Scribe Solutions. Any capitalized terms that are not otherwise defined in this Schedule “I” have the meanings ascribed to them in the Framework Agreement between the Vendor and Supply Ontario and in the Schedules to it.

1. Mandatory Provisions

These are the mandatory provisions applicable to the Purchasing Document between the Vendor and the Buyer, and shall be deemed to be part of the Purchasing Document. To the extent that there is any conflict between the provisions of the main body of the Purchasing Document or any Vendor terms, provisions, practices or policies (including the Vendor’s Standard T&Cs) or another schedule to the Purchasing Document, and these mandatory provisions, these provisions shall prevail.

The Vendor agrees that it will only access, use personal information (including personal health information as defined in the *Personal Health Information Protection Act* (Ontario)) (collectively, “**Personal Information**”) in accordance with the Requirements of Law and with the Purchasing Document, including these mandatory provisions. Vendor will provide the services enabled by the AI Scribe Solutions (the “**Services**”) to Buyer in accordance with the requirements of these mandatory provisions.

Buyer and its Authorized Users collect and process sensitive Personal Information using the Services. The Vendor agrees that it will not access, use or disclose Personal Information except in strict accordance with the Purchasing Document, including these mandatory provisions, and will provide the Services strictly in accordance with, and as constrained by, these mandatory provisions.

These mandatory provisions supersede and take precedence over any conflicting terms of use, agreement, privacy policy or end-user agreement of the Vendor and Vendor’s Standard T&Cs, even if there is a purported waiver of same by Buyer (which waiver is hereby acknowledged by Vendor and Buyer to be null and void), and shall govern the access, use, and disclosure of Personal Information.

In these mandatory provisions, unless defined elsewhere, the following words have the following meanings:

**“Electronic Service Provider”** means a person who supplies services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of PHI or PI and who is not a PHIPA Agent of the health information custodian;

**“health information custodian”** has the meaning ascribed to it in PHIPA;

**“PHIPA”** means the *Personal Health Information Protection Act*, *2004* (Ontario) and its regulations as amended from time to time; and

**“PHIPA Agent”** means an agent as defined in section 2 of PHIPA.

1. PHIPA Roles of the Vendor

Electronic Service Provider: Vendor and Buyer and its Authorized Users acknowledge and agree that, in providing certain of the Services Vendor will be acting only as an Electronic Service Provider and not a PHIPA Agent. As an Electronic Service Provider, Vendor will not:

1. use any Personal Information to which it has access in the course of providing the Services except as necessary in the course of providing the Services;
2. disclose any Personal Information to which it has access in the course of providing the Services to Buyer and its Authorized Users; or
3. permit its personnel to have access to the Personal information unless they agree to comply with the restrictions that apply to Vendor under these mandatory provisions.
4. Uses and Disclosures of Personal Information

(a) Performance of Services: Vendor will use Personal Information only for those purposes necessary to perform the Services and will not otherwise use or disclose such Personal Information.

(b) Training of Artificial Intelligence Systems: Vendor will not utilize Personal Information for any purpose other than as required to provide the Services, and will not permit the Personal Information, whether such Personal Information is de-identified or not, to be used for the purpose of training any system of Artificial Intelligence except for the sole benefit of the particular Buyer or Authorized User that is accountable for the use of the Personal Information.

(c) De-identification of Personal Information: Vendor will not de-identify Personal Information for any purpose, except if necessary and as limited by Section 2(b) above and except for purposes of creating a transcription and summary note as part of the Services, and acknowledges that de-identification for any other purpose is a use of Personal Information that is not authorized.

(d) Location of Personal Information: In performing the Services, Vendor shall store and process Personal Information only in Canada or, if outside Canada, with appropriate notice to Buyer (which shall include a statement that informs Buyer of their obligation to include this information in their publicly available privacy policy) and compliance with Requirements of Law and consent where required, in a location and with a cloud provider that complies with security requirements at least as strict as those required by the Purchasing Document, including these mandatory provisions.

1. Safeguards for Personal Information

(a) Reasonable Safeguards: Vendor will implement and maintain reasonable and appropriate safeguards to prevent any use or disclosure of Personal Information for purposes other than those permitted by the Purchasing Document, including administrative, physical and technical safeguards to protect the confidentiality, integrity, and availability of any Personal Information that Vendor creates, receives, maintains, or transmits on behalf of Buyer.

(b) Specific Requirements: Without limiting Vendor’s obligations in Section 4(a), Vendor shall at all times while processing Personal Information comply with the provisions of Section 9 below and shall destroy Personal Information in accordance with the provisions of Section 8 below.

(c) Data Backup and Disaster Recovery: Vendor will perform regular, automated backups of all data, including patient and other Personal Information, ensuring that backups are encrypted and stored in compliance with the requirements of Section 9 below, Requirements of Law, and industry best standards. Furthermore, Vendor will restore access to Personal Information and resume normal operations in a timely manner following a data loss incident, system failure, or other disaster.

1. Reports of Security Incidents and Privacy Breaches:

(a) For purposes of this Section 5, “**Security Incident**” means (i) accidental, unlawful or unauthorized disclosure of, access, destruction, loss, or alteration to Confidential Information or Personal Information; or, (ii) the Vendor’s system that stores and protects Confidential Information or Personal Information was compromised or system weaknesses were detected that may compromise the integrity of the Vendor’s system; and “**Privacy Breach**” means any unauthorized access to, use of, modification of, disclosure of, theft or loss of Personal Information or any collection, use or disclosure of Personal Information that is not permitted under Privacy Statutes or not otherwise permitted by the terms of this Agreement or required by law.

(b) Initial Reporting: Vendor will immediately report in writing (email) to Buyer and Authorized User (i) any actual or suspected Security Incidents, or (ii) any actual or suspected Privacy Breach, in either case upon Vendor’s learning of such Security Incident or such Privacy Breach.

(c) Supplementary Reporting: Vendor hereto recognizes that not all details of any particular Security Incident or Privacy Breach may be immediately available. Accordingly, Vendor shall report information concerning same without delay and in no event later than 48 hours, after it is discovered and provide additional reports thereafter as information is gathered. Upon request by Buyer, Vendor also will report the aggregate number of Privacy Breaches and Security Incidents in systems containing Personal Information, of which Vendor becomes aware.

(d) Interaction with Subjects: Vendor acknowledges that only the Authorized User accountable for Personal Information has the right to contact patients and other relevant individuals in the event of a Security Incident or Privacy Breach. Vendor shall provide reasonable assistance as required to Buyer for such purpose.

1. Access to Personal Information

(a) Access: Vendor will make Personal Information for which an Authorized User is accountable available to the Authorized User at all reasonable times in accordance with the Vendor’s obligations in the Purchasing Document. Vendor will never refuse or neglect to make Personal Information available to an Authorized User for any reason, including an alleged default by the Buyer.

(b) Individual Access or Amendment: If an individual makes a request for access to Personal Information or correction or Personal Information directly to Vendor, Vendor will within five (5) business days forward such request in writing to Buyer. Only Buyer or the applicable Authorized User will be responsible for making all determinations regarding the grant or denial of an individual’s request for Personal Information and the correction thereof and Vendor will make no such determinations. Only Buyer or the applicable Authorized User will release Personal Information to an individual pursuant to such a request.

1. Accounting of Disclosures of Personal Information

(a) Disclosure Records: Vendor will keep a record of any disclosures of Personal Information that Vendor makes where required by law. Vendor will maintain its record of such disclosures for seven (7) years from the date of the disclosure. This obligation does not obligate Vendor to maintain Personal Information beyond the period specified in Section 7 of this Schedule “I”.

(b) Data regarding Disclosures: For each disclosure for which it is required to keep a record under Section 7(a), Vendor will record and maintain the following information: (1) the date of disclosure; (2) the name of the entity or person who received the Personal Information and the address of such entity or person, if known; (3) the name and address of the person who is accountable for the Personal Information; (4) a description of the Personal Information disclosed (but without recording the Personal Information itself); and (5) a brief statement of the purpose of the disclosure.

1. Audit

Vendor will submit to an audit by Supply Ontario’s or Buyer’s auditor to validate continuing compliance with the data protection provisions and other requirements of the Purchasing Documents. Vendor will make its policies, procedures and records on the use and disclosure of Personal Information available for such purpose as reasonably required. Supply Ontario and Buyer may share the audit results with one another.

1. Destruction of Personal Information

(a) Routine Destruction of Personal Information: The processing Services provided by the Vendor include summarization of the patient encounter and the creation of summary notes in the nature of draft “SOAP” notes. The Authorized User reviews and approves the draft SOAP notes (with or without modification) and uploads them to their electronic medical record (“EMR”). Because the foregoing process involves the processing of sensitive Personal Information of both patient and Authorized User, it is essential that such Personal Information be rendered unrecoverable as soon as possible. Accordingly, the Vendor shall destroy the summarization of the patient encounter and all other Personal Information related to it as soon as the Authorized User has reviewed and approved the draft SOAP notes and uploaded them, with or without modification, to the EMR. There is no need for the Vendor to destroy any of the following information: (i) duration of sessions; (ii) number of characters transcribed or contained in a report; (iii) language of conversation and/or summarization; (iv) buttons clicked or functions selected to trigger any particular functionality; or (v) any other metadata that neither reveals any Personal Information nor can be combined with other information to reveal Personal Information.

(b) Destruction of Personal Information on Termination or Expiry: Upon termination or expiry of the Purchasing Document, Vendor will immediately return to the Buyer or Authorized User all Personal Information that Vendor or its subcontractors maintain in CSV format and PDF format, or such other format as reasonably requested by the Buyer or Authorized User. Immediately upon return of data, Vendor will, permanently destroy all such Personal Information and provide Buyer or Authorized User with written documentation confirming such destruction.

(c) Certificates of Destruction: A Certificate of Destruction must be provided by the Vendor at the request of Supply Ontario or the Buyer or Authorized User in the following circumstances:

(i) subject to Schedule “E”, on termination or expiry of the Purchasing Document, for the duration of the Purchasing Document; or

(ii) where there is any Security Incident or Privacy Breach being investigated, for the duration and scope of the engagement.

1. Specific Data Protection Requirements

(a) Administrative Safeguards

(i) Vendor shall implement and maintain a Privacy Breach and Security Incident reporting procedure to enable it to satisfy the reporting, recording, response, tracking, remediation, resolution and management reporting of Privacy Breaches and Security Incidents.

(ii) Vendor shall hold its individual managers accountable for ensuring that Services provided in their respective areas of responsibility are provided in a manner that complies with Vendor’s obligations under Requirements of Law and that respects privacy.

(iii) All Privacy Breaches and Security Incidents shall be documented promptly and submitted to the privacy officer of Vendor in accordance with Vendor’s Privacy Breach and Security Incident reporting procedure. Under the direction of Vendor’s privacy officer, any such breaches shall be handled collaboratively by Vendor and Buyer.

(iv) Vendor shall ensure that any employee or contractor repairing and maintaining a system which supports Vendor complies with the baseline requirements of Vendor’s security policy and its associated operational standards and technical documentation and with the requirements imposed upon Vendor under the Framework Agreement and any applicable Purchasing Document.

(v) Vendor shall provide its staff with appropriate annual training on security and privacy policies and security awareness and impose acceptable use guidelines.

(vi) Vendor shall limit access to its systems containing Personal Information to those of its employees or agents who specifically require such access to perform Services, and then only to the extent that such access is required.

(vii) Vendor shall ensure that individuals granted access to its systems containing or transmitting Personal Information are reliable and trustworthy and subject to binding obligations regarding safeguarding and non-disclosure of all Personal Information and other Confidential Information of Buyer that are at least as strict as those contained within the Schedule “E” (Non-OPS Entity Terms).

(b) Physical Safeguards

(i) All production systems that are part of the Vendor’s applications and other technology are secured using industry best practices and will comply with Requirements of Law. Such systems may be accessed only by Vendor personnel on a need-to-know basis and only via restricted and role-based access.

(ii) Vendor operations staff shall ensure that privacy and security are fully integrated early in the process of planning, selecting, designing and modifying technology (security by design).

(iii) Vendor shall ensure the secure storage, transmittal and disposal of Personal Information in all forms, in accordance with such physical security standards.

(iv) Vendor shall administer access to its systems through a user authentication database centrally maintained by Vendor. All Vendor users and others accessing Vendor’s systems and network shall be authorized and authenticated by Vendor.

(v) Vendor shall record every access by Vendor’s authorized personnel to Personal Information in an audit log, including the identity of the person who purported to access the information, the nature of the information accessed, and the time and date of access.

(vi) Vendor shall implement a file name nomenclature for Vendor that is designed to make it easier for Vendor operations staff to monitor end-to-end audit logs and to manage data in Vendor and related systems in a manner that will, to the extent possible, result in avoiding access to Personal Information.

(vii) Vendor shall conduct periodic security evaluations of systems, including assessments of configuration changes conducted on a routine basis, and shall make such evaluations and all other audit logs available to Buyer upon request.

(c) Technical Safeguards

(i) All data processed by the Vendor shall utilize end-to-end encryption, including protection (e.g., public key encryption, HL7/FHIR, TLS) for the Personal Information before storing it in the relevant secure electronic folders for access by Authorized Users.

(ii) Vendor shall annually provide Buyer with a copy of its SOC2 Type 2 Certificate for the ISO/IEC 27001/27002 compliant data centres that it uses for the processing and storage of Personal Information.

1. Limitations of Liability

The limitations of liability contained in Article15 of Schedule “E” (Non-OPS Entity Terms) form part of this Schedule “I” (Mandatory Provisions).