Information and Data Schedule for the provision of Surgery Intellect powered by TORTUS

Document

Document Status	**Live**
Document Author	Julian Coe
Issue Date	November 2025
Next Review Date	November 2026

Revision History

Version	Summary of Changes	Date
1.0	• Document Created	November 2025
1.1	• Further clarified the Controller, Processor, and Sub-processor roles • Specified data storage and retention protocols • Clarified on International transfers (LaunchDarkly) • Reworked the DPA to stand alone as the binding Article 28 UK GDPR agreement (in relation to DPIA).	April 2026

Authors

Version	Name	Title	Date
1.0	Julian Coe	Managing Director	November 2025
1.1	Julian Coe/Daniel Grainge	Managing Director/Product Assurance Officer	April 2026

Reviewers

Version	Name	Title	Date
1.0	Alice Reeves/Richard Newell	Solicitor/DPO	November 2025
1.1	Richard Newell	DPO	April 2026

Information and Data Schedule for the provision of Surgery Intellect powered by TORTUS

The Parties:	
The Authority and Data Controller	The end user of the Services who has contracted with the Supplier for the Services
The Supplier and Processor	**X-on Health Ltd** Glebe Farm Down Street, Dummer, Basingstoke, Hampshire, RG25 2AD Company Registration Number: 02578478

Recitals:

(1) The Processor has entered into a Subscription Agreement or Free Trial Agreement with the Authority (a "Subscription Agreement") in relation to the provision of 'Surgery Intellect powered by Tortus' (the "Services") which requires the Processor to process Personal Data on behalf of the Authority (the "Controller" or "Data Controller").

(2) Fundamental to the provision of the Services is the sub-contract of some of this processing to the Sub-Processor (Tortus AI Ltd, as defined below). The Processor and Sub-Processor have entered into a Software Subscription and Integration Agreement dated 2 July 2025 (the "Master Agreement"), and a data processing agreement which sets out the terms, requirements and conditions on which the Sub-Processor will Process Personal Data when providing services to the Processor under Subscription Agreement and the Master Agreement.

(3) This Schedule contains the mandatory clauses required by Article 28(3) of the UK GDPR and the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors which the Processor is required to flow-down to the Sub-Processor.

(4) The Authority and the Supplier undertake to comply with the provisions of this Schedule in the performance of their Subscription Agreement.

(5) Annex A details the Data Protection Protocol applicable to the provision of the Services.

(6) Annex B details the Data Privacy Impact Assessment applicable to the provision of the Services.

Definitions

Commencement Date	means the commencement date of the Subscription Agreement;
Confidential Information	means any information (whether written, oral, visual, electronic or in any other form) disclosed by one Party ("Discloser") to the other Party ("Recipient") in connection with this Schedule that is marked or otherwise identified as confidential, or that by its nature or the circumstances of disclosure ought reasonably to be treated as confidential. Confidential Information includes, without limitation: • all Personal Data and Sensitive Data;

	• business, financial, technical, operational, commercial or strategic information; • trade secrets, know-how, software, source code, algorithms, specifications, designs, drawings, and documentation; • information relating to patients, healthcare professionals, employees, contractors, or any third parties associated with the Discloser; • any reports, analyses, compilations, studies or other material prepared by the Recipient that contain or reflect such information; and excludes any information set out in Paragraph 1.1.2 of this Schedule.
Controller	shall have the same meaning as set out in the UK GDPR;
Data Protection Legislation	(a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data; and (b) To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Processor or Sub-Processor is subject, which relates to the protection of Personal Data;
Data Protection Officer	shall have the same meaning as set out in the UK GDPR;
Data Protection Impact Assessment or DPIA	means the Data Protection Impact Assessment detailed in Annex B;
Data Protection Protocol or Protocol	means the Data Protection Protocol detailed in Annex A;
Data Recipient	means that Controller who receives the relevant Personal Data;
Data Subject	shall have the same meaning as set out in the UK GDPR;
Data Subject Request	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
Data Security and Protection Toolkit	means the online self-assessment tool provided by NHS Digital that enables organisations to measure and demonstrate their compliance with data security and information governance standards required for handling NHS patient data;
Data Transferor	means that Controller who transfers the relevant Personal Data;
Information Commissioner	means the Information Commissioner in the UK;
Information Governance Policies	means the policies and standards provided by the Authority that set out requirements for the secure and lawful handling of Personal Data, including confidentiality, data protection compliance, information security, and records management

	in accordance with applicable law and NHS guidance;
Joint Controllers	means where two or more Controllers jointly determine the purposes and means of Processing;
National Security	means the protection of the United Kingdom, its people, institutions, and interests against threats that could compromise its sovereignty, territorial integrity, or democratic governance. This includes, but is not limited to, measures taken to prevent or respond to terrorism, espionage, sabotage, cyber-attacks, hostile state activity, or any other activity that poses a risk to the safety, defence, or security of the UK as defined under applicable laws, regulations, and government guidance;
Personal Data	shall have the same meaning as set out in the UK GDPR;
Personal Data Breach	shall have the same meaning as set out in the UK GDPR;
Processor	shall have the same meaning as set out in the UK GDPR;
Sensitive Data	shall mean the types of data set out in Article 9(1) or 10 of the UK GDPR;
Sub-Processor or Sub-Contractor	Means TORTUS AI Ltd (Company Registration number: 14487060) or any other third Party appointed to Process Personal Data on behalf of the Processor;
UK GDPR	has the meaning given in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1 **Confidentiality**

1.1 In respect of any Confidential Information it may receive directly or indirectly from the Discloser and subject always to the remainder of Paragraph 1 of this Schedule, each Recipient undertakes to keep secret and strictly confidential and shall not disclose any such Confidential Information to any third party without the Discloser's prior written consent provided that:

1.1.1 the Recipient shall not be prevented from using any general knowledge, experience or skills which were in its possession prior to the Commencement Date;

1.1.2 the provisions of Paragraph 1 of this Schedule shall not apply to any Confidential Information:

(i) which is in or enters the public domain other than by breach of this Schedule or other act or omissions of the Recipient;

(ii) which is obtained from a third party who is lawfully authorised to disclose such information without any obligation of confidentiality;

(iii) which is authorised for disclosure by the prior written consent of the Discloser;

(iv) which the Recipient can demonstrate was in its possession without any obligation of confidentiality prior to receipt of the Confidential Information from the Discloser; or

(v) which the Recipient is required to disclose purely to the extent to comply with the requirements of any relevant stock exchange.

1.2 Nothing in Paragraph 1 of this Schedule shall prevent the Recipient from disclosing Confidential Information where it is required to do so by judicial, administrative, governmental or regulatory process in connection with any action, suit, proceedings or claim or otherwise by applicable law.

1.3 The Authority may disclose the Supplier's Confidential Information:

1.3.1 on a confidential basis to NHS England organisations;

1.3.2 on a confidential basis, to any consultant, contractor or other person engaged by the Authority for receiving such information;

1.3.3 on a confidential basis to any relevant party for the purpose of the examination and certification of the Authority's accounts;

1.3.4 to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirements; or

1.3.5 on a confidential basis to a proposed successor body in connection with any proposed or actual, assignment, novation or other disposal of rights, obligations, liabilities or property in connection with this Schedule;

and for the purposes of this Schedule, references to disclosure "on a confidential basis" shall mean the Authority making clear the confidential nature of such information and that those individuals and/or organisations set out under this Paragraph 1.3 of this Schedule are under binding confidentiality obligations no less onerous than set out in Paragraph 1 of this Schedule.

1.4 The Supplier may only disclose the Authority's Confidential Information, and any other information provided to the Supplier by the Authority in relation to this Schedule and/or the Subscription Agreement, to the Supplier's staff or professional advisors who are directly involved in the performance of or advising on the Supplier's obligations under this Schedule and the Subscription Agreement. The Supplier shall ensure that such staff or professional advisors are aware of and shall comply with the obligations in Paragraph 1 of this Schedule as to confidentiality and that all information, including Confidential Information, is held securely, protected against unauthorised use or loss and, at the Authority's written discretion, destroyed securely or returned to the Authority when it is no longer required. The Supplier shall not, and shall ensure that the staff do not, use any of the Authority's Confidential Information received otherwise than for the purposes of performing the Supplier's obligations in this Schedule and the Subscription Agreement.

1.5 For the avoidance of doubt, save as required by law or as otherwise set out in this Schedule, the Supplier shall not, without the prior written consent of the Authority (such consent not to be unreasonably withheld or delayed), announce that it has entered into this Schedule and/or that it has been appointed as a Supplier to the Authority and/or make any other announcements about this Schedule.

1.6 Paragraph 1 of this Schedule shall remain in force:

1.6.1 without limit in time in respect of Confidential Information which:

(i) comprises Personal Data, but shall continue for only as long as the Processor or Sub-Processor holds or has access to any such Personal Data; or

(ii) which relates to National Security; and

for all other Confidential Information for a period of three (3) years after the expiry or earlier termination of the Subscription Agreement unless otherwise agreed in writing by the Parties.

2 Information Security

2.1 Without limitation to any other information governance requirements set out in this Schedule, the Supplier shall:

2.1.1 notify the Authority forthwith of any information security breaches or near misses (including without limitation any potential or actual breaches of confidentiality or actual information security breaches) in line with the Authority's Information Governance Policies; and

2.1.2 fully cooperate with any audits or investigations relating to information security and any privacy impact assessments undertaken by the Authority and shall provide full information as may be reasonably requested by the Authority in relation to such audits, investigations and assessments.

2.2 The Supplier will ensure that it puts in place and maintains an information security management plan appropriate to the type of Services being provided and the obligations placed on the Supplier. The Supplier shall ensure that such plan is consistent with any relevant and applicable policies, guidance, good industry practice and with any relevant quality standards as may be set out by the NHS.

2.3 The Supplier and Sub-Processor shall obtain and maintain certification under the HM Government Cyber Essentials Scheme.

3 Data protection

3.1 The Parties acknowledge their respective duties under Data Protection Legislation and shall give each other all reasonable assistance as appropriate or necessary to enable each other to comply with those duties. For the avoidance of doubt, the Parties shall take reasonable steps to ensure they are familiar with the Data Protection Legislation and any obligations they may have under such Data Protection Legislation and shall comply with such obligations.

3.2 Where the Supplier is Processing Personal Data and/or the Parties are otherwise sharing Personal Data under or in connection with this Schedule and the Subscription Agreement, the Parties shall comply with the Data Protection Protocol in respect of such matters.

3.3 The Supplier and the Authority shall ensure that patient related Personal Data is safeguarded at all times in accordance with the Data Protection Legislation, and this obligation will include (if transferred electronically) only transferring patient related Personal Data (a) if essential, having regard to the purpose for which the transfer is conducted; and (b) that is encrypted in accordance with any international data encryption standards for healthcare, and as otherwise required by those standards applicable to the Authority under any law and guidance (this includes, data transferred over wireless or wired networks, held on laptops, CDs, memory sticks and tapes).

3.4 Where, as a requirement of the Services, the Supplier is Processing Personal Data relating to NHS patients and/or service users and/or has access to NHS systems as part of the Services, the Supplier shall:

3.4.1 complete and publish an annual information governance assessment using the Data Security and Protection Toolkit;

3.4.2 achieve all relevant requirements in the relevant Data Security and Protection Toolkit;

3.4.3 nominate an information governance lead able to communicate with the Supplier's board of directors or equivalent governance body, who will be responsible for information governance and from whom the Supplier's board of directors or equivalent governance body will receive regular reports on information governance matters including, but not limited to, details of all incidents of data loss and breach of confidence;

3.4.4 report all incidents of data loss and breach of confidence in accordance with Department of Health and Social Care and/or the NHS England and/or Health and Social Care Information Centre guidelines;

3.4.5 put in place and maintain policies that describe individual personal responsibilities for handling Personal Data;

3.4.6 put in place and maintain a policy that supports its obligations under the NHS Care Records Guarantee (being the rules which govern information held in the NHS Care Records Service, which is the electronic patient/service user record management service providing authorised healthcare professionals access to a patient's integrated electronic care record);

3.4.7 put in place and maintain agreed protocols for the lawful sharing of Personal Data with other NHS organisations and (as appropriate) with non-NHS organisations in circumstances in which sharing of that data is required under this Schedule and/or the Subscription Agreement;

3.4.8 where appropriate, have a system in place and a policy for the recording of any telephone calls in relation to the Services, including the retention and disposal of those recordings;

3.4.9 comply with any new and/or updated requirements, guidance and/or policies notified to the Supplier by the Authority from time to time (acting reasonably) relating to the Processing and/or protection of Personal Data.

3.5 Where any Personal Data is Processed by the Sub-processor or any other sub-contractor of the Supplier, the Supplier shall procure that such Sub-contractor shall comply with the relevant obligations set out this Schedule and any relevant Data Protection Protocol, as if such Sub-contractor were the Supplier.

3.6 Subject to any cap or limitation on the Supplier's liability set out in the Subscription Agreement, the Supplier shall indemnify and keep the Authority indemnified against, any loss, damages, costs, expenses (including without limitation legal costs and expenses), claims or proceedings whatsoever or howsoever arising from the Supplier's unlawful or unauthorised Processing, destruction and/or damage to Personal Data in connection with this Schedule.

3.7 The Data Protection Protocol applies to the Authority and the Supplier.

Annex A

DATA PROTECTION PROTOCOL

IMPORTANT NOTE ON DOCUMENT STRUCTURE:

This Protocol, Table A, and the Schedule constitute the binding controller–processor arrangement between the parties for the purposes of Article 28 UK GDPR.

The Controller's own practice-specific DPIA remains a separate controller document. It is not incorporated into this Agreement and is not a condition of its operation or interpretation.

Annex B contains the Supplier's DPIA and related technical materials, provided for reference and supporting information only. Nothing in Annex B shall amend, override, or be used to interpret the obligations in this Protocol or Table A. In the event of any conflict, this Protocol and Table A shall prevail.

Readers seeking further background on the technical architecture, data flows, or security measures may refer to Annex B for reference. Such reference is optional and does not affect the interpretation of the parties' contractual obligations.

Table A – Processing, Personal Data and Data Subjects

SUMMARY OF DATA PROCESSING ROLES

This Data Protection Protocol governs an integrated solution comprising:

1. Telephony and call management services (provided by X-on Health as Processor);
2. AI-assisted clinical documentation services (provided by Tortus AI as Sub-Processor).

KEY DISTINCTIONS:

Details - X-on Health (PROCESSOR)	
Role	Call routing, telephony infrastructure, call management
Data Processed	Call metadata, telephone numbers, timestamps
Data Stored	**YES** – X-on Health may retain call metadata and associated telephony service records, and where applicable call recordings, in accordance with the agreed retention schedule and applicable NHS records management requirements. The Practice clinical system / EHR remains the primary system of record and stores the finalised patient note and any approved clinical correspondence.
Storage Location	Secure UK data centres
Certifications	ISO 27001, ISO42001, DTAC ready, Cyber Essentials Plus, DSPT *Standards Exceeded*

Details - Tortus AI (SUB-PROCESSOR)

Role	Real-time AI transcription, summarisation, clinical coding
Data Processed	Consultation audio (real-time only), patient identifiers (transiently, for EHR integration)
Data Stored	NO – Tortus AI processes consultation audio and related inputs to generate draft outputs for clinician review and does not retain consultation audio, transcripts, or clinical outputs beyond live processing, other than temporary session or browser memory cleared on logout or within 24 hours where applicable
Processing Model	Browser-based, real-time processing with immediate output to Controller's EHR
Certifications	UKCA Class I Medical Device, ISO 27001, DTAC ready, Cyber Essentials Plus, DSPT *Standards Exceeded*, DCB0129 compliant

CRITICAL PRIVACY SAFEGUARD:

The Practice clinical system / EHR remains the primary system of record and stores the finalised patient note and any approved clinical correspondence. X-on Health may retain call metadata and associated telephony service records, and where applicable call recordings, in accordance with the agreed retention schedule and applicable NHS records management requirements. Tortus AI processes consultation audio and related inputs to generate draft outputs for clinician review and does not retain consultation audio, transcripts, or clinical outputs beyond live processing, other than temporary session or browser memory cleared on logout or within 24 hours where applicable. Audit, access and support logs may be retained by the relevant processor or sub-processor only for legitimate security, support, monitoring and compliance purposes and in accordance with the agreed retention and deletion arrangements.

DATA FLOW OVERVIEW:

1. Patient contacts practice via X-on Health telephony system;
2. Clinician conducts consultation using Tortus AI-powered documentation tool;
3. Audio processed in real-time within clinician's browser (local processing);
4. AI outputs written directly to Controller's EHR;
5. Tortus AI retains nothing; browser memory cleared after 24h/logout;
6. X-on Health retains only call metadata per retention schedule.

Further technical detail is available for reference in Annex B, which is provided as supporting information only and does not form part of this Agreement

X-on Health personnel cannot access Tortus AI systems or clinical data processed by the Sub-Processor.

Table A	
Description	**Detail**
Subject matter of the Processing	The provision of the Services by the Supplier to the Authority to transcribe, summarise and code conversations between the Authority's staff and patients.
Duration of the Processing	For the duration of the Subscription Agreement between the Supplier and the Authority.
Nature and purposes of the Processing	The Services support the provision of direct care to patients by registered health and care professionals through an integrated telephony and AI-assisted documentation solution. PROCESSOR ROLE (X-on Health): X-on Health provides telephony services including call routing, contact management, and call recording. Processing operations include collection, recording, storage, retrieval, and transmission of call data and metadata. SUB-PROCESSOR ROLE (Tortus AI): Tortus AI provides real-time AI transcription, summarisation, and clinical coding services during patient consultations. Processing operations include real-time speech-to-text conversion, AI-assisted summarisation, and generation of clinical documentation. CRITICAL DISTINCTION - DATA RETENTION: The Practice clinical system / EHR remains the primary system of record and stores the finalised patient note and any approved clinical correspondence. X-on Health may retain call metadata and associated telephony service records, and where applicable call recordings, in accordance with the agreed retention schedule and applicable NHS records management requirements. Tortus AI processes consultation audio and related inputs in real time to generate draft outputs for clinician review and does not retain consultation audio, transcripts, or clinical outputs beyond live processing, other than temporary session or browser memory cleared on logout or within 24 hours where applicable. Audit, access and support logs may be retained by the relevant processor or sub-processor only for legitimate security, support, monitoring and compliance purposes and in accordance with the agreed retention and deletion arrangements. DATA FLOW: 1. Patient consultation audio is captured during the clinical encounter;

	2. Audio is processed in real-time by Tortus AI within the clinician's browser; 3. AI-generated outputs (transcriptions, summaries, clinical codes) are written directly to the Controller's Electronic Health Record (EHR) system; 4. Tortus AI retains no copies of audio, transcripts, or outputs; 5. Temporary processing memory in the browser is automatically cleared after 24 hours or upon user logout, whichever occurs first; 6. Call metadata (timestamps, duration) is retained by X-on Health as specified below. Processing operations include but are not limited to: collection, recording, organisation, structuring, storage (by X-on only), adaptation, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment, restriction, erasure and destruction of data for the purposes defined by the Controller. No patient data is stored by the Sub-Processor (Tortus AI). All clinical information remains under the exclusive control of the Controller within their clinical system.
Type of Personal Data	Patient identifiers required for patient matching and filing; consultation audio; consultation content; generated draft transcript, summary, note, letter and coding output; call metadata where applicable; staff identifiers required for authentication and support; and audit / access / support log data. Special category data will primarily comprise health data disclosed during the consultation. Personal, Special and Confidential Information: Sensitive Data processed will be determined by the Controller but will primarily comprise health data relevant to a GP consultation. All Sensitive data processed will, in compliance with Article 9 of the UK GDPR, be subject to restrictions or safeguards that fully take into consideration the nature of the data and the risks involved including strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data and restrictions for onward transfers. Criminal Offence data may also be processed.
Categories of Data Subject	Patients of the Authority; clinicians and authorised Authority staff using the service; and any incidental third-party individuals whose information may be mentioned during a consultation where clinically relevant.

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data	DATA RETENTION BY PROCESSOR (X-on Health): The Practice clinical system / EHR remains the primary system of record and stores the finalised patient note and any approved clinical correspondence. X-on Health may retain call metadata and associated telephony service records, and where applicable call recordings, in accordance with the agreed retention schedule and applicable NHS records management requirements. Tortus AI processes consultation audio and related inputs in real time to generate draft outputs for clinician review and does not retain consultation audio, transcripts, or clinical outputs beyond live processing, other than temporary session or browser memory cleared on logout or within 24 hours where applicable. Audit, access and support logs may be retained by the relevant processor or sub-processor only for legitimate security, support, monitoring and compliance purposes and in accordance with the agreed retention and deletion arrangements. This is done in accordance with: - The contractually agreed retention period between the Controller and Processor; - NHS Records Management Code of Practice for Health and Social Care 2021 (Updated 2023); - The Controller's own data retention policy. The Code of Practice advises the transfer of relevant information from call recordings into the main health record through transcription or summarisation. Where it is not possible to transfer the clinical information from the recording to the health record, the recording must be considered part of the record and retained accordingly. Upon expiry or termination of the Agreement, the Processor shall, at the Controller's choice, securely return or securely delete personal data held on behalf of the Controller, and provide certifications of deletion, except to the extent that continued retention is required by law or by agreed records management obligations. Nothing in this clause shall override the Controller's legal and professional obligations relating to the retention of clinical records. All data deletion is performed using secure methods that prevent recovery.
Technical and organisational measures **for the Processor** including technical and organisational measures to ensure the security of the data	X-on Health (the Processor) implements the following technical and organisational measures to ensure the security of call data and telephony metadata: CERTIFICATIONS AND COMPLIANCE: • ISO 27001 certified - Data held in secure UK data centres. • ISO 42001 certified. • ISO 14001 certified. • ISO 22301 certified. • ISO 9001 certified. • NHS Digital Technology Assessment Criteria (DTAC ready). • ICO registration (Z8221333).

	• NHS Data Security and Protection Toolkit (DSP Toolkit)- 'Standards Exceeded' (ODS Code: 8JM42). • Cyber Essentials Plus Certification. • DCB0129 Clinical Risk Management compliance. SECURITY CONTROLS: • End-to-end encryption for data in transit (TLS 1.3). • Encryption at rest (AES-256). • Multi-factor authentication (MFA) and Single Sign-On (SSO). • Role-based access control (RBAC). • Regular penetration testing (annual minimum) by CREST-approved testers with all identified vulnerabilities remediated. • Regular access audits and monitoring. • Mandatory staff security awareness training. DATA MINIMISATION: • Telephone numbers (non-sensitive personal identifiers) are not associated with patient names or other personal identifiers within the telephony system. • Patient lookup to EHR retrieves only: name, date of birth, and Patient ID. • Name and date of birth remain locally within the application. • Only Patient ID is stored against phone call records. • Any patient identifier or system identifier capable of being linked back to an identifiable individual, whether directly or through other information reasonably available to the parties, shall be treated as personal data for the purposes of this Agreement. ACCESS RESTRICTIONS: • X-on Health personnel CANNOT access Tortus AI systems, or any clinical data processed by the Sub-Processor. • X-on Health personnel have no access to consultation audio, transcripts, summaries, or AI-generated clinical documentation. • Access to telephony metadata is restricted to authorized personnel only.
Processor's Technical and Organisational measures for assistance to the Controller	The Processor shall assist the Controller in compliance with Articles 32–36 UK GDPR through the following measures: 1. Security Information Provision: o Provide documentation of implemented security controls (e.g., encryption standards, access controls, penetration testing reports). o Share ISO 27001 certification and DSP Toolkit compliance evidence annually.

	2. Data Protection Impact Assessment (DPIA) Support: o Supply detailed descriptions of processing activities, data flows, and risk mitigations. o Provide technical architecture diagrams and security risk assessments upon request. 3. Consultation with ICO - Cooperate with the Controller in preparing information required for prior consultation under Article 36, including technical safeguards and residual risk analysis. 4. Incident Response: o Maintain and share breach response procedures. o Provide logs and forensic data to support risk evaluation and mitigation planning. 5. Timelines for Assistance - Respond to Controller requests for assistance within 5 business days for standard requests and 24 hours for urgent matters (e.g., breaches or ICO consultations). The Processor's assistance shall be limited to providing information and cooperation reasonably required for compliance, based on the nature of the processing and the information available to the Processor. The Processor shall not be responsible for performing the Controller's legal obligations or for costs beyond reasonable administrative effort.
Technical and organisational measures **for the Sub-Processor** including technical and organisational measures to ensure the security of the data	Tortus AI (the Sub-Processor) implements the following technical and organisational measures. NOTE: Due to Tortus AI's zero-retention architecture, these measures focus on securing data in transit and during real-time processing only: CERTIFICATIONS AND COMPLIANCE: • ISO 27001 certified. • UKCA-marked Class I Medical Device (pursuing Class IIa certification). • NHS Digital Technology Assessment Criteria (DTAC ready). • DCB0129 Clinical Risk Management compliance. • NHS Ambient Voice Technology (AVT) Instructions compliant. • ICO registration (ZB512995). • NHS Data Protection and Security Toolkit - 'Standards Exceeded' (ODS Code: 8HF76). • Cyber Essentials Plus Certification. AUTHENTICATION AND ACCESS: • User authentication aligned with Gov.uk and NIST

	standards. • Multi-factor authentication (MFA). • Single Sign-On (SSO) integration with NHS Identity systems. • Role-based access control (RBAC). DATA IN TRANSIT SECURITY: • All data securely transmitted via HTTPS, WSS, SSL/TLS 1.3. • End-to-end encryption between clinician browser and Tortus AI services. • Secure API connections to Controller's EHR systems - Annual penetration testing (minimum) incorporating 'data in transit' within scope. • All identified vulnerabilities remediated before production release. ZERO-RETENTION ARCHITECTURE: • Real-time processing model: audio processed immediately and discarded. • No audio files stored at any time. • No transcripts stored at any time. • No clinical summaries or AI outputs stored at any time. • All outputs written directly to Controller's EHR system only. • Temporary browser-based processing memory automatically cleared after: 24 hours (maximum) or user logout (whichever occurs first). PERSONNEL ACCESS CONTROLS: Tortus AI personnel access to production systems strictly controlled: • Personnel may have incidental access to Controller staff identifiers (usernames, email addresses) for backend administration purposes only. • Personnel CANNOT access consultation data (audio, transcripts, summaries, clinical outputs) as these are not stored in Tortus systems. • All personnel subject to confidentiality obligations and security training. INTERNATIONAL TRANSFERS: Limited use of LaunchDarkly (US-based feature flag platform) for Tortus AI controlled feature releases. LaunchDarkly is certified under UK-US Data Privacy Framework. No patient or clinical data is transferred to LaunchDarkly. Only non-identifiable feature flags and user IDs are transmitted, which does not constitute as personal data. The Processor shall ensure that no patient or clinical data is transferred outside the UK unless expressly authorised in writing by the Controller and supported by a lawful transfer mechanism under Chapter V UK GDPR. Where a third-country service is used for

	limited non-clinical functionality, the Processor shall identify the data transferred, confirm whether it constitutes personal data, identify the applicable transfer safeguard, and notify the Controller in advance of any material change to that transfer mechanism. MONITORING AND TESTING: • Continuous security monitoring; • Regular vulnerability assessments; • Annual penetration testing by CREST-approved testers; • Automated security scanning in development pipeline. The Sub-Processor's security model is designed around the principle that data which doesn't exist cannot be breached. By storing no clinical data whatsoever, Tortus AI eliminates the most significant data protection risks. Further technical detail on the Sub-Processor's architecture is available for reference in Annex B, which is provided as supporting information only and does not form part of this Agreement.
Personal Data Breach notification obligations - **Processor's assistance in case of Personal Data Breach**	The Processor shall provide the following information and support to the Controller upon becoming aware of a Personal Data Breach: 1. Description of the Breach - Nature of the breach, including categories and approximate number of Data Subjects affected and Personal Data records concerned. 2. Contact Point - Details of a designated contact person for further information regarding the breach. 3. Consequences - Likely consequences of the breach for Data Subjects and the Controller. 4. Mitigation Measures - Measures taken or proposed to address the breach and mitigate its possible adverse effects. 5. Timeline for Updates - Initial report within 24 hours of awareness, followed by regular updates until resolution. 6. Supporting Documentation - Relevant logs, audit trails, and technical reports necessary for the Controller to notify the Information Commissioner and affected Data Subjects under Articles 33 and 34. 7. Cooperation - Cooperation with the Controller in drafting notifications to the ICO and Data Subjects. The Processor's assistance shall be limited to providing information and cooperation reasonably required for compliance, based on the nature of the processing and the information available to the Processor. The Processor shall not be responsible for performing the Controller's legal obligations or for costs beyond reasonable administrative effort.

1 Supplier as data processor

1.1 **Purpose and scope**

1.1.1 The purpose of this Clause 1 is to ensure compliance with Article 28(3) and (4) of the UK GDPR.

1.1.2 This Clause 1 applies to the Processing of Personal Data as specified in Table A.

1.1.3 Table A is an integral part of this Clause 1.

1.1.4 This Clause 1 is without prejudice to obligations to which the Controller is subject by virtue of the UK GDPR.

1.1.5 This Clause 1 does not by itself ensure compliance with obligations related to international transfers in accordance with Chapter V of the UK GDPR.

1.2 **Invariability of Clause 1**

1.2.1 The Parties undertake not to modify Clause 1, except for adding information to Table A or updating information in it by mutual agreement.

1.2.2 This does not prevent the Parties from including the standard contractual clauses laid down in this Clause 1 in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict Clause 1 or detract from the fundamental rights or freedoms of Data Subjects.

1.3 **Interpretation**

1.3.1 Where this Clause 1 uses the terms defined in the UK GDPR, those terms shall have the same meaning as in the UK GDPR.

1.3.2 This Clause 1 shall be read and interpreted in the light of the provisions of the UK GDPR.

1.3.3 This Clause 1 shall not be interpreted in a way that runs counter to the rights and obligations provided for in the UK GDPR or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.

1.4 **Hierarchy**

1.4.1 In the event of a contradiction between this Schedule and the provisions of the Subscription Agreement, this Schedule shall prevail.

1.5 **Description of the processing**

1.5.1 The details of the Processing operations, in particular the categories of Personal Data and the purposes of Processing for which the Personal Data is Processed on behalf of the Controller, are specified in Table A.

1.6 **Obligations of the Parties**

1.6.1 <u>Instructions</u>

(i) The Processor shall Process Personal Data only on documented instructions from the Controller, unless required to do so by law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before Processing, unless the law prohibits this on important grounds of public interest. Subsequent

instructions may also be given by the Controller throughout the duration of the Processing of Personal Data. These instructions shall always be documented.

(ii) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe the UK GDPR.

1.6.2 Purpose Limitation

(i) The Processor shall Process the Personal Data only for the specific purpose(s) of the Processing, as set out in Table A, unless it receives further instructions from the Controller.

1.6.3 Duration of the Processing of Personal Data

(i) Processing by the Processor shall only take place for the duration specified in Table A.

1.6.4 Security of Processing

(i) The Processor shall at least implement the technical and organisational measures specified in Table A to ensure the security of the Personal Data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for the Data Subjects.

(ii) The Processor shall grant access to the Personal Data undergoing Processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Subscription Agreement. The Processor shall ensure that persons authorised to Process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

1.6.5 Sensitive Data

(i) If the Processing involves Sensitive Data as set out in Table A, or data relating to criminal convictions and offences, the Processor shall apply specific restrictions and/or additional safeguards as agreed between the Parties in Table A.

1.6.6 Documentation and compliance

(i) The Parties shall be able to demonstrate compliance with this Clause 1.

(ii) The Processor shall deal promptly and adequately with inquiries from the Controller about the Processing of data in accordance with this Clause 1.

(iii) The Processor shall make available to the Controller all relevant information necessary to demonstrate compliance with the obligations that are set out in this Clause 1 and stem directly from the UK GDPR (being records, systems, and facilities directly related to the Processing

of Personal Data under this Schedule and the Subscription Agreement). At the Controller's request, the Processor shall also permit and contribute to audits of the Processing activities covered by this Clause 1, at reasonable intervals being no more than once a year, or if there are indications of non-compliance. In deciding on a review or an audit, the Controller shall take into account relevant certifications held by the Processor.

(iv) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor and shall, be carried out on no less than fourteen (14) days' notice from the Controller to the Processor.

(v) The Parties shall make the information referred to in this Clause 1, including the results of any audits, available to the Information Commissioner on request.

(vi) Audits shall be carried out during normal business hours and in a manner that minimises disruption to the Processor's business operations.

(vii) Each Party shall bear its own costs for audits.

(viii) The Controller shall ensure that any auditor (whether they are an employee, agent or contractor of the Controller, or an independent auditor) is bound by confidentiality obligations and shall not disclose any information obtained during the audit except as required by law or regulatory authority.

1.6.7 Use of Sub-processors

(i) The Controller consents to the subcontract of Processing operations to the Sub-Processor, TORTUS AI as detailed above.

(ii) The Processor has engaged the Sub-Processor to carry out specific Processing activities (on behalf of the Controller) as detailed in Table A, by way of a data processing agreement which imposes on the Sub-Processor, in substance and to the extent relevant, the same data protection obligations as the ones imposed on the Processor in accordance with this Clause 1. The Processor shall ensure that the Sub-Processor complies with the obligations to which the Processor is subject pursuant to this Clause 1 and to the UK GDPR

(iii) The Processor shall not subcontract any of its Processing operations performed on behalf of the Controller in accordance with this Clause 1 to any other Sub-Processor, without the Controller's prior specific written authorisation (not to be unreasonably withheld or delayed). The Processor shall submit the request for specific authorisation at least fourteen (14) days prior to the engagement of a Sub-Processor in question, together with the information necessary to enable the Controller to decide on the authorisation.

(iv) At the Controller's request, the Processor shall provide a copy of the Sub-Processor data processing agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including Personal Data, the Processor may redact the text of the data processing

agreement prior to sharing the copy.

(v) Subject to any cap or limitation on the Processor's liability as set out in the Subscription Agreement, the Processor shall remain fully responsible to the Controller for the performance of the Sub-Processor's obligations in accordance with its data processing agreement with the Processor. The Processor shall notify the Controller of any failure by the Sub-Processor to fulfil its contractual obligations.

1.6.8 International Transfers

(i) The Controller agrees to the international transfer in respect of the use of LaunchDarkly. This feature flag platform software which is hosted in the US is used to release features to specific users for testing purposes. No patient or clinical data is transferred to LaunchDarkly and LaunchDarkly is certified under the UK-US Data Privacy Framework.

(ii) The Processor shall ensure that no patient or clinical data is transferred outside the UK unless expressly authorised in writing by the Controller and supported by a lawful transfer mechanism under Chapter V UK GDPR. Where a third-country service is used for limited non-clinical functionality, the Processor shall identify the data transferred, confirm whether it constitutes personal data, identify the applicable transfer safeguard, and notify the Controller in advance of any material change to that transfer mechanism.

(iii) Any other transfer of data to a third country or an international organisation by the Processor shall be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under law to which the Processor is subject and shall take place on the basis of an adequacy regulation (in accordance with Article 45 of the UK GDPR) or standard data protection clauses (in accordance with Article 46 1 the UK GDPR). All such transfers shall comply with Chapter V of the UK GDPR and any other applicable Data Protection Legislation.

(iv) The Controller agrees that where the Processor engages a Sub-Processor in accordance with Clause 1.6.7. for carrying out specific Processing activities (on behalf of the Controller) and those Processing activities involve a transfer of Personal Data within the meaning of Chapter V of GDPR, the Processor and the Sub-Processor can ensure compliance with Chapter V of the UK GDPR by using standard contractual clauses adopted by the Information Commissioner in accordance with Article 46(2) of the UK GDPR, provided the conditions for the use of those standard contractual clauses are met.

1.7 **Assistance to the Controller**

1.7.1 The Processor shall promptly notify the Controller if it receives a Data Subject Request. The Controller shall deal with and respond to any such Data Subject Request.

1.7.2 The Processor shall assist the Controller in fulfilling its obligations to respond to Data Subject Requests to exercise their rights, taking into account the nature of the Processing. In fulfilling its obligations in accordance with Clauses

1.7.1 and 1.7.3 the Processor shall comply with the Controller's reasonable instructions.

1.7.3 In addition to the Processor's obligation to assist the Controller pursuant to Clause 1.7.2, the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data Processing and the information available to the Processor:

(i) the obligation to carry out a Data Protection Impact Assessment where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;

(ii) the obligation to consult the Information Commissioner prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

(iii) the obligation to ensure that Personal Data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the Personal Data it is Processing is inaccurate or has become outdated; and

(iv) the obligations in Article 32 of the UK GDPR.

1.7.4 The Parties shall set out in Table A the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Clause 1.7 as well as the scope and the extent of the assistance required.

1.8 **Notification of Personal Data Breach**

1.8.1 In the event of a Personal Data Breach, the Processor shall co-operate with and assist the Controller to comply with its obligations under Articles 33 and 34 of the UK GDPR, where applicable, taking into account the nature of Processing and the information available to the Processor.

1.8.2 <u>Personal Data Breach concerning data Processed by the Controller</u>

In the event of a Personal Data Breach concerning data Processed by the Controller, the Processor shall reasonably assist the Controller:

(i) in notifying the Personal Data Breach to the Information Commissioner, without undue delay after the Controller has become aware of it, where relevant, and where feasible, within 72 hours of becoming aware of a breach, (unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(ii) in obtaining the following information which, pursuant to Article 33(3) of the UK GDPR, shall be stated in the Controller's notification, and must at least include:

(A) the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

(B) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(C) the likely consequences of the Personal Data Breach; and

(D) the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. The Controller shall document any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken.

(iii) in complying, pursuant to Article 34 of the UK GDPR, with the obligation to communicate without undue delay the Personal Data Breach to the Data Subject, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

1.8.3 Personal Data Breach concerning data Processed by the Processor

(i) In the event of a Personal Data Breach concerning data Processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

(A) a description of the nature of the breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);

(B) the details of a contact point where more information concerning the Personal Data Breach can be obtained; and

(C) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. The Controller shall document any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken.

(ii) The Parties shall set out in Table A all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under Articles 33 and 34 of the UK GDPR.

1.9 **Non-compliance with Clause 1 and termination**

1.9.1 Without prejudice to any provisions of the UK GDPR, in the event that the Processor is in breach of its obligations under this Clause 1, the Controller may instruct the Processor to suspend the Processing of Personal Data until it

complies with this Clause 1, or until the Subscription Agreement is terminated in accordance with Clause 1.9.2 below. The Processor shall not be liable to the Controller for any consequences arising from its suspending such Processing at the Controller's instruction. For the avoidance of doubt, any suspension of Processing under this Clause 1.9.1 shall be deemed a suspension of the Services, and the Processor shall not be considered in breach of the Subscription Agreement or any associated service level commitments as a result of such suspension. The Controller shall remain liable for all fees and charges during any period of suspension unless otherwise agreed in writing. The Processor shall promptly inform the Controller in case it is unable to comply with this Clause 1 for whatever reason.

1.9.2 The Controller shall be entitled to terminate the Subscription Agreement insofar as it concerns Processing of Personal Data in accordance with this Clause 1 if:

(i) the Processing of Personal Data by the Processor has been suspended by the Controller pursuant to Clause 1.9.1 and if compliance with this Clause 1 is not restored within a reasonable time and in any event within one month following suspension;

(ii) the Processor is in substantial or persistent breach of this Clause 1 or its obligations under the UK GDPR;

(iii) the Processor fails to comply with a binding decision of a competent court or the Information Commissioner regarding its obligations pursuant to this Clause 1 or to the UK GDPR.

1.9.3 The Processor shall be entitled to terminate the Subscription Agreement insofar as it concerns Processing of Personal Data under this Clause 1 where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 1.6.1(ii), the Controller insists on compliance with the instructions.

1.9.4 Following termination of the Subscription Agreement, the Processor shall, at the instructions of the Controller, delete all Personal Data Processed on behalf of the Controller and certify to the Controller that it has done so, or, return all the Personal Data to the Controller and delete existing copies unless the law requires storage of the Personal Data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with this Clause 1.

2 Parties as joint controllers

2.1 Not applicable.

3 Both data controllers

3.1 Not applicable

4 Changes to this protocol

4.1 Any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.

Annex B

SUPPLIER'S DATA PROTECTION IMPACT ASSESSMENT

The current version of the applicable DPIA can be found on the X-on Health Trust Centre at https://surgeryconnect.academy/wp-content/uploads/2025/06/Overarching-Data-Protection-Impact-Assessment-DPIA.pdf

The current version at the date of contract signature is attached:

Annex B Surgery Intellect Data-Protecti