X-ON HEALTH

SERVICE SCHEDULE FOR SURGERY INTELLECT

Your attention is particularly drawn to Clauses 3.3-3.4 (inclusive), 12.2- 12.3 (inclusive) and Clause 19 (Limitation of Liability)

Please read this Service Schedule in conjunction with the Supplier's Master Services Agreement and Privacy Notice which can be found on any of the Supplier Website.

The Supplier's Master Services Agreement, which has been accepted by the Customer, applies to this Service Schedule.

1. DEFINITIONS AND INTERPRETATION

1.1 In this service schedule (**Service Schedule**) the following words shall have the following meanings and other defined terms shall have the same meaning as set out in the Master Services Agreement:

Authorised Users	means any employee, agent, independent contractor or self-employed partner of the Customer authorised to access and use the Goods, Services and Documentation in accordance with this Contract, provided that: (a) for User Subscription Licence Customers, the number of such users does not exceed the number of User Subscriptions purchased pursuant to Clause 6, and (b) for Enterprise Licence Customers, such users are employed or engaged by the Customer at the Permitted Practice(s), and in each case meet the requirements set out in Clause 5.
Best Practice	means the exercise of that degree of skill, care, prudence and foresight which would reasonably and ordinarily be expected from a competent organisation operating in the same or similar circumstances, in accordance with applicable laws, regulatory requirements, relevant NHS standards (including DCB0129 and DCB0160), and recognised industry guidance.
Cap	has the meaning given to it under Clause 19.4(c).
Charges	means the charges payable by the Customer to the Supplier for the Goods and Services, as specified in the Quotation and subject to adjustment in accordance with Clauses 6.4 and 6.5 of the Master Services Agreement and/or as otherwise permitted under the Contract.
Clinical Safety Requirements	means maintaining UKCA Class I Medical Device approved and DCB0129 compliance
Contract Year	a 12 month period commencing on the Effective Date or any anniversary of it.

Customer Computer System	databases, software, cabling, systems, computer hardware, networks and any other components to the Customer's computer system owned or used by the Customer (excluding those elements provided to the Customer by the Supplier as part of the Services);
Customer Default	has the meaning given to it under Clause 12.5;
Customer Equipment	any Equipment not supplied by the Supplier that is used by the Customer to access the Goods and Services. Any Equipment the Customer purchases from the Supplier shall also be considered to be Customer Equipment once title has passed to the Customer pursuant to Clause 5.8 of the Master Services Agreement.
Customer Usage Data	means data and content generated from or relating to the Customer's use of the Services, including audio, video, text, metadata, metrics, statistics and technical or performance information from calls, meetings or conversations processed by the Service, including aggregated and statistical data;
Documentation	any document(s) and other materials made available to the Customer by the Supplier online via https://help.x-onweb.com/en/collections/794299-surgery-intellect-powered-by-tortus or such other web address notified by the Supplier to the Customer from time to time which sets out a description of the Services and the user instructions for the Services.
Fault	a reproducible malfunction, defect or failure in the Goods or Services that adversely affects the quality, performance, functionality, or continuity of the Goods or Services that is not a Technology Limitation;
Installation Services	means the installation, configuration and related implementation services provided by the Supplier prior to the Actual Services Commencement Date, as more particularly described in Clause 9 and Schedule 3;
International Destination Network	a network operated in an overseas country;
Master Services Agreement	the Supplier's Master Services Agreement made available to the Customer at the Supplier's website at www.x-on.co.uk/terms/
NavBar	has the meaning given to it under Clause 4.2;
Overage Charge	means the charge payable by the Customer for usage exceeding the Usage Threshold, calculated by reference to the

	Overage Rate and the number of hours consumed in excess of the Usage Threshold, whether by an individual practice (in respect of Customers subscribed to the Enterprise Licence) or per User Subscription (for Customers subscribed to the User Subscription Licence), in accordance with Clause 14.2.
Overage Rate	means the rate set out in the Quotation.
Patient	any individual who are registered with, or receiving care from, the Customer or any Authorised User, and who may be the subject of the Services.
Patient Data	any information, content, material or data relating to the health, care, treatment, or medical condition of a Patient which may be stored, processed, used, generated or relied on by Surgery Intellect.
Permitted Practice(s)	the care practice(s) specified in the Quotation,
Services	the provision of access to Surgery Intellect which has the functionality and specification set out in Schedule 1, together with the Support Services detailed in Schedule 2 by the Supplier to the Customer under the Contract
Service Levels	The service levels set out in Schedule 2 applicable to the provision of Support Services.
Software	the software programs and applications supplied under the Contract, including all updates, upgrades and modifications, and includes the installation, configuration, customisation, interfacing and integration of such software into the Customer's Computer System to ensure its proper operation within that system
Support Services	support services provided by the Supplier or its appointed third party, including: (a) responding to reasonable enquiries relating to the Service; and (b) remote diagnosis and, where possible, correction of faults using the software management tools, as further described in Schedule 2 (Help Desk Service Levels).
Supplier Website	means the Supplier's Website available at URL: https://www.x-on.co.uk/;
Surgery Connect Contract	the terms and conditions which sets out the service-specific terms applicable to Surgery Connect;
Surgery Intellect	a software solution for use by medical professionals that transcribes spoken language into written text, creates clinical notes and referral letters and files these notes to the electronic

	health record (as further described in the specification set out in Schedule 1).
Surgery Intellect Output	means any and all information, data, materials, content, text, images, audio, video, software code, works, expressions, communications, notes, reports, or other outputs, whether in tangible or intangible form, that are generated, derived, produced or otherwise created, in whole or in part, by or through the use of Surgery Intellect.
Technology Limitation	means the inherent limitations of the Services and underlying technologies, including any Surgery Intellect Output, or other outputs generated by the Services, may from time to time be inaccurate, incomplete, misleading, or otherwise not factually correct.
Termination Sum	the amount payable by the Customer to the Supplier upon early termination of the Contract pursuant to Clause 20.1 of the Master Services Agreement and Clause 15.2 of this Service Schedule, calculated as an amount equal to seventy five per cent (75%) of the fees and charges that would have been payable by the Customer for the remainder of the agreed Initial Term had the Contract not been terminated early prior to expiry of the Initial Term, excluding any amounts already paid.
Usage Threshold	the agreed permitted volume of audio transcription usage per month for the Customer's use of the Service, being: (i) in respect of a User Subscription, the number of hours of audio transcription allocated per subscribed user; and (ii) in respect of an Enterprise Subscription, the number of hours of audio transcription allocated per registered patient, in each case as specified in the Quotation.
User Subscriptions	the individual user subscriptions purchased by the Customer from the Supplier pursuant to Clause 6, in respect of Customers subscribed to the User Subscription Licence only, which entitle Authorised Users to access and use the Services and the Documentation in accordance with the Contract.
Virus	any thing or device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme

	or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.
Vulnerability	a weakness in the computational logic (for example, code) found in software and hardware components that when exploited, results in a negative impact to the confidentiality, integrity, or availability of Customer Input, and/or the Services, and the term **Vulnerabilities** shall be interpreted accordingly.
Warranty Period	has the meaning given to it under clause 10.5.

2. MASTER SERVICES AGREEMENT

2.1 This Service Schedule incorporates the terms of the Master Services Agreement. For the avoidance of doubt, in the event of conflict between the Master Services Agreement and the terms of this Service Schedule, the terms of this Service Schedule shall prevail.

2.2 Expressions defined in the Master Services Agreement and used in this Service Schedule have the meaning set out in the Master Services Agreement unless otherwise defined.

2.3 The rules of interpretation set out in the Master Services Agreement apply to this Service Schedule.

2.4 The Contract constitutes the entire agreement between the parties in respect of its subject matter. The Customer acknowledges that it has not relied on any statement, promise, representation, assurance or warranty the Supplier has made or given, or which has been made or given on the Supplier's behalf which is not set out in the Contract.

2.5 The Contract shall govern the Goods and Services provided under this Service Schedule to the exclusion of any other terms that the Customer seeks to impose or incorporate, or which are implied by trade, custom, practice or course of dealing.

3. SUPPLY OF SERVICES

3.1 The Supplier shall, during the Term, provide the Services including the Support Services and make available the Documentation to the Customer on and subject to the terms of the Contract (as defined under the Master Services Agreement).

3.2 The Supplier shall use commercially reasonable endeavours to make the Services available 24 hours a day, seven days a week, except for:

(a) planned maintenance carried out during the maintenance window of 10:00 pm to 2:00 am UK time; and

(b) any unscheduled maintenance carried out following advance notice to the Customer, where giving such notice is technically feasible.

3.3 Surgery Intellect is a medical device (as defined under the UK Medical Devices Regulations 2002) but it is not intended to assess, diagnose, treat, cure, or prevent any disease or medical condition or prescribe any medication. The Service does not provide medical advice, and any Surgery Intellect Output must be reviewed and verified by a qualified healthcare professional before being used in clinical decision-making or patient records.

3.4 Use of the Service does not substitute professional judgment or clinical oversight. The Service is provided solely as a transcription and documentation support tool and must not be relied upon for clinical assessment or treatment planning.

3.5 The Supplier may modify or update the Goods, Services, Software or Documentation at any time by providing notice to the Customer, provided that such changes do not materially impair the Customer's ability to access or use the core functionality of the Services subject always to any downtime or disruption caused by scheduled or unscheduled maintenance as permitted under Clause 3.2 or usage limits set by the Supplier as permitted under Clause 3.6.

3.6 The Supplier reserves the right to implement reasonable usage limits and traffic management measures to ensure system stability, provided that such measures are applied proportionally and do not unreasonably restrict agreed Service Levels or reduce the Customer's permitted usage below the applicable Usage Threshold.

3.7 The Customer accepts and acknowledges that:

(a) the Supplier shall not be liable or responsible for any delays, delivery failures or any loss or damage arising out of or resulting from the transfer of data including but not limited to Customer Input or Customer Usage Data, over communications Networks and facilities (including the internet) unless directly caused by an act or omission of the Supplier;

(b) the Services may be subject to limitations, delays, interruptions, and other issues inherent in the use of communications networks and infrastructure, including but not limited to internet connectivity and third-party telecommunications systems;

(c) scheduled downtime will occur from time to time. The Supplier will use its reasonable endeavours to provide the Customer with at least three (3) Working Days' notice of any scheduled downtime. Although the Supplier will not be responsible for any loss or consequence of delay suffered by the Customer arising out of any scheduled or unscheduled downtime in the Services, it will use all reasonable endeavours within its control to prevent or reduce such downtime;

(d) the existence of any minor errors or interruptions in the Services shall not constitute a breach of the Contract by the Supplier;

(e) Customer Usage Data may be used to train, improve, test and refine the Service's algorithms and models, provided such use does not result in the disclosure of Customer confidential information; and

(f) Technical Limitations are inherent in, and a well-recognised characteristic of, current artificial intelligence technologies, including those incorporated within the Software and Services, and that the Customer agrees to receive and use the Software and Services on that basis.

3.8 The Customer acknowledges and agrees that the Supplier and/or its licensors own all Intellectual Property Rights in the Software, Goods, Service and any related Documentation. The Contract does not grant the Customer any rights to, or in, patents, copyrights, database rights, trade secrets, trade names, trade marks (whether registered or unregistered), or any other rights or licences in respect of the Software, Services or any related Documentation.

3.9 The Customer acknowledges and accepts that no warranties or undertakings are provided as to the content or quality of the Documentation and the Supplier has no obligation to update the Documentation or provide further Documentation, including to adapt it to the Customer's use or satisfaction.

3.10 The Supplier shall not be obliged to investigate or fix any Fault if the Fault is directly or indirectly caused by the Customer's:

(a) failure to comply with any user manual or other Documentation made available by the Supplier relating to the Service;

(b) failure to follow any oral or written instructions issued by the Supplier regarding the use or operation of the Services;

(c) use of the Services in a manner that is not in accordance with the documentation, specifications, or intended purpose as described by the Supplier, including but not limited to unauthorised modification, misuse, or use with incompatible equipment or software;

(d) breach of the Contract by the Customer; or

(e) use of the Services for purposes, in environments, or in connection with equipment or systems for which the Services were not designed, specified, or intended by the Supplier.

3.11 If the Supplier agrees, at its discretion, to investigate, fix or attend to a Fault:

(a) caused by the circumstances described in Clause 3.10;

(b) directly or indirectly caused by an act or omission of the Customer;

(c) that otherwise falls outside the responsibility of the Supplier; or

(d) where, upon investigation, no Fault is found,

then the Supplier may charge the Customer for such work at its prevailing standard man-hour rates.

4. TELEPHONY SERVICES

4.1 The Software within the Services provides outbound call functionality. For Customers who also purchase Surgery Connect from the Supplier, the Services are fully integrated into Surgery Connect and the provision of the telephony functionality is governed by the Surgery Connect Contract.

4.2 Where the Customer is not a Surgery Connect paid user, the Services include the softphone functionality detailed in Schedule 1 Annex B (**NavBar**) and this aspect of the Service is governed by Surgery Connect Contract currently in force.

4.3 In the event of conflict between the terms of this Service Schedule and the Surgery Connect Contract, the terms of this Service Schedule shall prevail.

4.4 Inbound call transcription shall only be available where Surgery Connect is the paid telephony platform selected by the Customer and is provided by the Supplier. Inbound call transcription shall not be provided where Surgery Connect is not the Customer's paid telephony platform of choice or is not supplied by the Supplier.

5. AUTHORISED USERS

5.1 The Customer shall not permit any third party other than the Authorised Users to access or use the Goods and Services except with the prior written consent of the Supplier, which may be withheld or granted subject to conditions.

5.2 In relation to the Authorised Users, the Customer undertakes that:

(a) each Authorised User is fully licensed and registered with the General Medical Council, or otherwise authorised to provide patient care to individuals in the UK;

(b) it shall permit the Supplier or the Supplier's designated auditor to audit the Services in order to establish the name of each Authorised User and the Customer's data processing facilities to audit compliance with the Contract. The Supplier's right to audit pursuant to this Clause 5.2(b) shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Customer's normal conduct of business;

(c) if any audit conducted pursuant to clause 5.2(b) reveal that the Service has have been used or accessed by any individual who is not an Authorised User or granted a User Subscription pursuant to the terms of the Contract, then without prejudice to the Supplier's other rights, the Customer shall promptly disable such use or access; and

(d) if any of the audits conducted pursuant to Clause 5.2(b) reveal that the Customer has underpaid the Charges to the Supplier, then without prejudice to the Supplier's other rights, the Customer shall pay to the Supplier an amount equal to such underpayment as calculated in accordance with the Charges within 15 calendar days of the date of the relevant audit.

5.3 The Customer shall not, and procure that each Authorised User does not, access, store, introduce, distribute or transmit any Viruses or Vulnerabilities, or any material, during the course of its use of the Services that:

(a) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

(b) facilitates illegal activity;

(c) depicts sexually explicit images;

(d) promotes unlawful violence;

(e) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or

(f) is otherwise illegal or causes damage or injury to any person or property;

and the Supplier reserves the right, without liability to the Customer or prejudice to its other rights to the Customer, to disable the Customer's access to any material that breaches the provisions of this Clause.

5.4 The Customer shall not and procure that each Authorised User does not:

(a) except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties and except to the extent expressly permitted under this Service Schedule:

(i) attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of Surgery Intellect, the Software, the Goods, the Service and/or Documentation (as applicable) in any form or media or by any means; or

(ii) attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of Surgery Intellect, the Software or the Service;

(b) access all or any part of the Services and Documentation in order to build a product or service which competes with Surgery Intellect, Goods, Services and/or the Documentation;

(c) subject to Clause 21, license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Goods, Services and/or Documentation available to any third party, except the Authorised Users to the extent permitted under the licences granted under Clause 6 or Clause 7 (as the case may be);

(d) attempt to obtain, or assist third parties in obtaining, access to the Goods, Services and/or Documentation, other than as provided under this Clause 5;

(e) introduce or permit the introduction of, any Virus or Vulnerability into Surgery Intellect, the Services or the Supplier's network and information systems or the network and information systems of the Supplier's third party suppliers or subcontractors from time to time; or

(f) delegate final clinical decision-making to Surgery Intellect;

(g) use of the Service outside of its patient care practice or approved device, such as on personal devices or non-integrated applications; or

(h) use the Goods, Services and/or Documentation to provide services to third parties except as expressly permitted under the Contract.

5.5 The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Goods, Service and/or the Documentation and, in the event of any such unauthorised access or use, immediately notify the Supplier in writing.

6. USER SUBSCRIPTION LICENCE

6.1 Where specified in the Quotation, and subject to the Customer (i) purchasing the number of User Subscriptions set out in the Quotation (ii) complying with the restrictions set out in this Clause 6, and (iii) complying with the other terms of this Service Schedule, the Supplier grants to the Customer a non-exclusive, non-transferable, revocable and non-sublicensable licence to permit Authorised Users to access and use the Goods, Services and Documentation on a User Subscription basis for the Term solely for the purposes of the Customer's patient care practice, subject to the terms of the Contract.

6.2 The Customer undertakes that the maximum number of Authorised Users that it authorises to access and use the Goods, Services, Software and the Documentation shall not exceed the number of User Subscriptions it has purchased from time to time.

6.3 Subject to Clause 6.4 and Clause 6.5, the Customer may, from time to time during the Term, purchase additional User Subscriptions in excess of the number set out in the Quotation and the Supplier may grant access to the Goods, Services and the Documentation to such additional Authorised Users in accordance with the provisions of this Service Schedule.

6.4 If the Customer wishes to purchase additional User Subscriptions, the Customer shall notify the Supplier in writing. The Supplier shall evaluate such request for additional User Subscriptions and respond to the Customer with approval or rejection of the request (such approval not to be unreasonably withheld). Where the Supplier approves the request, the Supplier shall activate the additional User Subscriptions within one (1) Business Day of its approval of the Customer's request.

6.5 If the Supplier approves the Customer's request to purchase additional User Subscriptions, the Customer shall pay to the Supplier the relevant fees for such additional User Subscriptions in accordance with Clause 14 and, if such additional User Subscriptions are purchased by the

Customer part way through the Term, such fees shall be pro-rated from the date of activation by the Supplier for the remainder of the Term.

6.6 In relation to User Subscriptions, the Customer's access to the Goods and Services shall be limited to the number of individual User Subscriptions specified in the Quotation together with any additional User Subscriptions purchased by the Customer during the Term in accordance with the Contract, and the Customer shall not permit the Goods and Services to be accessed by more individuals than that number. User Subscriptions may not be shared or transferred between users except with the prior written consent of the Supplier.

7. ENTERPRISE LICENCE

7.1 Where specified in the Quotation and subject always to the Customer complying with its obligations under this Service Schedule, the Customer shall be granted a non-exclusive, non-transferable, revocable and non-sublicensable licence to access and use the Goods, Services and Documentation on an Enterprise Licence basis for the Term, solely for the purposes of the Customer's patient care practice at the Permitted Practice(s).

7.2 The rights granted to the Customer under this Clause 7 in respect of the Enterprise Licence are limited to the Permitted Practice(s). The Customer shall not permit the Goods, Services or Documentation to be accessed or used at, or for the benefit of, any other care practice, location or premises without the Supplier's prior written consent and agreement to any applicable additional Charges.

7.3 The Charges for the Enterprise Licence shall be calculated by reference to the number of patients registered at the Permitted Practice(s) as at the Effective Date, as recorded in the Quotation. Such Charges shall be invoiced and payable in accordance with Clause 14. For the avoidance of doubt, any subsequent increase or decrease in the number of patients shall not result in any adjustment to the Charges payable during the Term.

7.4 Under the Enterprise Licence, an unlimited number of Authorised Users employed or engaged by the Customer, whose primary place of work is at the Permitted Practice(s), may access and use the Goods, Services and Documentation during the Term, subject to payment of the applicable Charges

8. SUPPORT SERVICES

8.1 The Supplier will, as part of the Services and at no additional cost to the Customer provide the Customer with the Supplier's standard customer Support Services during Business Hours.

9. INSTALLATION SERVICES

9.1 Prior to commencement of the provision of the Services and/or delivery of Goods, the Customer acknowledges and accepts that there is an installation and implementation process to be completed

by the Supplier. The standard implementation requirements are detailed in this Clause 9 and Schedule 3 (Implementation Process), and the Supplier may impose additional implementation requirements from time to time as it reasonably considers necessary for the delivery of the Goods and Services, by written notice to the Customer. Any dates specified by the Supplier for installation are intended to be an estimate only and time shall not be of the essence for delivery and/or any of the Supplier's obligations under the Contract and shall not be made of the essence by notice. The Supplier will make reasonable efforts to meet any performance dates agreed between the parties, but where no dates are so specified, delivery of the Goods and/or provision of Services will be within a reasonable time.

10. GOODS RELATED SERVICES AND WARRANTY

10.1 The Supplier reserves the right to substitute the Goods detailed in the Quotation with compatible models of an equivalent or superior type in the event of issues arising in the availability of the Goods.

10.2 Goods that experience an irreparable Fault during the Warranty Period may be replaced by Supplier via a next Business Day courier service. This will typically be phones, handsets, headsets, connecting leads or mobile devices. The Customer should report such failures to Supplier's Customer Services Department, providing the information listed under paragraph 1 of Schedule 2 (Help desk service levels) . Once the need for replacement equipment is diagnosed by the Supplier's Staff, a replacement will be dispatched to the Customer within 8 Business Hours. The Customer will be emailed an equipment return label (including postage) to return the faulty Goods to the Supplier.

10.3 The warranty given by Supplier under Clause 10.2 above shall not apply, and any replacement Goods provided by the Supplier will be charged to the Customer in line with Supplier's then current price list, if:

(a) the repair or replacement is required as a result of any accident, neglect, misuse, tampering with, or unauthorised modification of the Goods by or on behalf of the Customer outside of the manufacturer's or Supplier's recommendations;

(b) interference with the Goods by persons other than the Supplier Staff; or

(c) supplies from sources which have not been authorised by Supplier are used in the Goods.

10.4 Supplier provides no warranty and makes no guarantees for suitability of third party telecommunications devices and services for use with the Services that are purchased outside this Contract.

10.5 Goods purchased by the Customer become the property of the Customer on receipt of payment in full by the Supplier. In respect of these Goods, the Supplier warrants to the Customer that these Goods shall be free of defects in workmanship and materials for the period of 24 months after dispatch to the Customer (**Warranty Period**). If such a defect arises within the Warranty Period in

respect of the Goods of one or more of its component parts, the Supplier will either repair or replace the defective Goods or component in accordance with the Contract.

11. RESPONSIBILITIES OF THE SUPPLIER

11.1 The Supplier shall perform the Services and Support Services with reasonable skill and care.

11.2 The Supplier's obligations under the Contract shall not apply to the extent of any non-conformance which is caused by use of the Services in breach of the terms of the Contract or contrary to the Supplier's instructions, or modification or alteration of the Services by the Customer or any party other than the Supplier or the Supplier's duly authorised contractors, agents or suppliers. If the Supplier fails to perform Services or Support Services in accordance with Clause 11.1, the Supplier will, at its expense, use reasonable commercial endeavours to correct any such non-conformance within a reasonable timeframe.

11.3 The Supplier warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under the Contract, specifically:

(a) the Supplier warrants that the Software and Services will comply with Annex A of Schedule 4 (Quality Standards)

(b) the Supplier warrants that the Software and Services will comply with the Clinical Safety Requirements.

11.4 The Supplier does not warrant that:

(a) the Customer's use of the Services or Support Services will be uninterrupted or error-free; or

(b) that the Goods, Services, Documentation and/or the information obtained by the Customer through the Services will meet the Customer's specific requirements or is accurate; or

(c) that the Software or the Services will be free from Vulnerabilities, Viruses or Technical Limitations.

11.5 The Supplier does not warrant that the Surgery Intellect Output is accurate, complete, or suitable for use in connection with the Customer’s patient care practice. It is the sole responsibility of the Customer to assess, and to procure its Authorised Users to assess, the appropriateness and reliability of any Surgery Intellect Output for any intended clinical purpose. The Supplier shall have no liability arising from any reliance placed on Surgery Intellect Output in the course of providing medical services or otherwise.

11.6 The Contract shall not prevent the Supplier from entering into similar agreements with third parties, or from independently developing, using, selling or licensing documentation, products and/or services which are similar to those provided under this Service Schedule.

12. CUSTOMER'S OBLIGATIONS

12.1 The Customer shall:

(a) provide the Supplier with:

(i) all necessary co-operation in relation to the Contract; and

(ii) all necessary access to such information as may be required by the Supplier,

in order to provide the Services and Support Services, including but not limited to Customer Input, security access information and configuration services;

(b) without affecting its other obligations under the Contract, comply with all applicable laws including sanctions laws and regulations with respect to its activities under the Contract including without limitation in relation to their use of the Services;

(c) be responsible for maintaining compliance with DCB0160 and shall ensure that all clinical safety matters arising from or in connection with its use of the Goods and Services are properly identified, managed and addressed in accordance with Best Practice and relevant clinical risk management standards.

(d) carry out all other Customer responsibilities set out in the Contract in a timely and efficient manner. In the event of any delays in the Customer's provision of such assistance as agreed by the Parties, the Supplier may adjust any agreed timetable or delivery schedule as reasonably necessary and the Supplier shall not be liable for any failure or delay to deliver any or all of the Services to the extent caused by Customer’s delay;

(e) ensure that the Authorised Users use the Goods, Services, Support Services, Software and the Documentation in accordance with the terms and conditions of the Contract and shall be responsible for any Authorised User's breach of the Contract;

(f) ensure that Customer Computer System, IT infrastructure and connectivity are adequately maintained at all times and remain sufficient to enable the Supplier to efficiently provide the Services;

(g) ensure that the Supplier shall have such remote and other access to the Customer Computer System and infrastructure of the Customer to the extent necessary to provide the Services;

(h) enter into and maintain contracts directly with such third party providers as may be necessary to enable the Supplier to provide the Services;

(i) ensure that any Software, Documentation or manuals (if any) provided by the Supplier to the Customer to enable the Customer to receive and use the Goods and Services, are used for the Customer’s patient care practice only and, except as permitted by applicable law or as expressly permitted under the Contract the Customer will not, without the Supplier’s prior written consent, copy, de-compile, distribute or modify any Software, nor copy the manuals or documentation relating to that Software, nor knowingly allow or permit anyone else to do so;

(j) not use the Goods and Services and will take all reasonable steps to ensure that the Goods and Services are not used by anyone:

(i) to send, knowingly receive, upload, download, use or re-use material which is offensive, indecent, defamatory, obscene or menacing;

(ii) in a way that does not comply with the terms of any legislation or any licence applicable to the Customer;

(iii) in a manner that is in any way unlawful, fraudulent or in bad faith or, to the knowledge of the Customer, has any unlawful, fraudulent or bad faith purpose or effect; and

(k) maintain adequate security measures to protect the Services from unauthorised access or use.

12.2 The Customer and each Authorised User shall be responsible for checking and verifying any Surgery Intellect Output generated from its use of the Service, Software and/or Documentation. The Supplier shall have no responsibility to the Customer in respect of the Customer's use of Surgery Intellect Output, including, without limitation, any matters arising from the Customer's patient care practice (including without limitation the sale or provision of medical or patient care services), irrespective of whether such services were informed by, or based upon, the Surgery Intellect Output (in whole or in part).

12.3 The Customer is solely responsible for ensuring the accuracy, legality, quality, integrity of Customer Input.

12.4 The Customer shall not, and shall ensure that its Authorised Users do not, attempt to gain unauthorised access to the Goods and Services or engage in any activity that disrupts, degrades, or interferes with the performance or integrity of the Goods and Services, or that otherwise prevents the Supplier from fulfilling its obligations under this Contract or any other agreement it has entered into with any third party.

12.5 If the Supplier's performance of any of its obligations under the Contract is prevented or delayed by any act or omission by the Customer or failure by the Customer to perform any relevant obligation (**Customer Default**):

(a) the Supplier shall without limiting its other rights or remedies, have the right to suspend performance of the Goods and Services until the Customer remedies the Customer Default, and to rely on the Customer Default to relieve it from the performance of any of its obligations to the extent the Customer Default prevents or delays the Supplier's performance of any of its obligations;

(b) the Supplier shall not be liable for any costs or losses sustained or incurred by the Customer arising directly or indirectly from the Supplier's failure or delay to perform any of its obligations under the Contract; and

(c) the Customer shall reimburse the Supplier on written demand for any costs or losses sustained or incurred by the Supplier arising directly or indirectly from the Customer Default.

12.6 The Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Customer Input except to the extent caused by the Supplier's negligence. Notwithstanding any other provision, the Supplier shall be entitled (but not obliged) to remove and/or delete (in the Supplier's absolute discretion) any Customer Input which it considers breaches the Customer's obligations under the Contract.

12.7 The Customer is solely responsible for backing up all Customer Input submitted to or generated whilst using or engaging with Surgery Intellect. The Supplier does not retain or store Customer Input beyond what is necessary to provide the Service. In the event of any loss or damage to Customer Input, the Customer's sole and exclusive remedy shall be for the Supplier to provide reasonable commercial assistance to restore such Customer Input, where possible.

12.8 From the moment the Surgery Intellect Output is generated, the Supplier shall not be responsible for any loss, permanent erasure, or inability to use or access Surgery Intellect Output. The Customer acknowledges and agrees that it is solely responsible for ensuring that all Surgery Intellect Output is stored in a secure and accessible location, and that it can be retrieved for future use or reference as required by the Customer. The Supplier disclaims all liability in relation to the storage, retention, and accessibility of Surgery Intellect Output from the point of its creation.

12.9 The Customer shall not utilise and shall ensure that no other person uses the Goods, Services or Documentation:

(a) for storing, reproducing, transmitting, communicating or receiving any material in breach of any law, regulation, code of practice; or

(b) fraudulently or for any criminal or illegal purpose or in a manner that is contrary to any regulatory or legal requirement; or

(c) for any defamatory, offensive, obscene, indecent, menacing, abusive, nuisance or hoax purposes; or

(d) to cause annoyance, inconvenience or needless anxiety to any person; or

(e) contrary to instructions that the Supplier may give to the Customer from time to time; or

(f) to copy, store, modify, publish or distribute services or content (including ringtones), except where the Supplier gives the Customer prior permission in writing; or

(g) to download, send or upload content of an excessive size, quantity or frequency. The Supplier will contact the Customer if the Customers use is excessive; or

(h) in violation of any applicable local, national, or international law or regulation; or

(i) in any way which may damage the reputation of the Supplier; or

(j) in a manner which infringes the rights of any person, including intellectual property rights and rights of confidentiality

13. DATA PROTECTION AND INFORMATION GOVERNANCE

13.1 The Parties shall comply with their respective obligations under Schedule 5 (Information Governance and Data Protection) of this Service Schedule.

13.2 The Parties acknowledge that the Customer is the Controller and the Supplier is the Processor in respect of Personal Data Processed under this Contract.

13.3 When the Customer records communication, it is their responsibility to ensure that all parties in the communication are informed and any necessary consent is provided. The Customer shall inform all parties that the communication may or will be recorded.

13.4 The Customer consents to the Supplier appointing TORTUS as a third-party processor of Personal Data under this Service Schedule. The Supplier confirms that it has entered or (as the case may be) will enter with the third-party processor into a written agreement incorporating terms which are substantially similar to those set out in this Clause 13.

13.5 Subject to clause 13.6, the Supplier may collect, store and use Customer Usage Data for the purposes of:

(a) managing, administering, and delivering the Services;

(b) improving and developing the Services;

(c) complying with its obligations under this Agreement;

(d) providing support and maintenance services; and

(e) understanding how the Services are used.

13.6 The Supplier shall not use any Personal Data to train AI models, but may use anonymised usage patterns, performance metrics and non-patient-identifying data to improve and refine Surgery Intellect.

13.7 If the Customer or Authorised User takes payment details from a patient on a call it is their responsibility to ensure their practice on call recording is appropriate pursuant to applicable Data Protection Laws including without limitation:

(a) maintaining accurate and clear records of any such information disclosed;

(b) ensuring confidentiality of the information provided;

(c) securely storing or deleting any records of such information in accordance with its own obligations under applicable data protection laws; and

(d) taking all required steps to prevent unauthorised access, disclosure, or misuse of such information.

14. CHARGES AND PAYMENT

14.1 The Customer shall pay the Charges to the Supplier for the User Subscriptions, Enterprise Subscription Licence and Overage Charges in accordance with this Clause 14 and Clause 12 of the Master Services Agreement.

14.2 The Supplier shall invoice the Customer for any hours of audio transcription services consumed in excess of the Usage Threshold (the **Overage Charge**), with such Overage Charges calculated at the applicable Overage Rate. For this purpose, Customer usage is measured by the Supplier's systems and records, which shall be final in the absence of manifest error. The Customer shall pay all Overage Charges in accordance with this Clause 14.

14.3 On the Effective Date, the Customer shall provide to the Supplier valid, up-to-date and complete direct debit details and any other relevant billing information. The Customer authorises the Supplier to collect payment by direct debit on a monthly basis as follows:

(a) the first payment shall be collected 15 calendar days after the Actual Services Commencement Date and shall include: (i) all Charges for Services and/or Goods (including any Implementation Services) provided up to the last day of the first calendar month following the Actual Services Commencement Date; and (ii) Charges payable in advance for the provision of the Services and/or Goods for the following calendar month; and

(b) thereafter, Charges shall be collected monthly in advance by direct debit in respect of each calendar month during the Term.

14.4 If the Supplier has not received payment within 30 days after the due date, and without prejudice to any other rights and remedies of the Supplier:

(a) the Supplier may, on no less than five (5) Business Days' notice to the Customer and without liability to the Customer, disable the Customer's password, account and access to all or part of the Services and/or Goods and the Supplier shall be under no obligation to provide any or all of the Services and/or Goods while the invoice(s) concerned remain unpaid; and

(b) interest shall accrue on a daily basis on such due amounts at an annual rate equal to 4% over the then current base lending rate of the Supplier's bankers in the UK from time to time, commencing on the due date and continuing until fully paid, whether before or after judgment, but at 4% a year for any period when that base rate is below 0%.

14.5 All amounts and fees stated or referred to in this Contract:

(a) shall be payable in pounds sterling;

(b) are exclusive of value added tax, which shall be added to the Supplier's invoice(s) at the appropriate rate.

14.6 The provision of the Services and delivery of the Goods are conditional on the Customer entering into a Direct Debit agreement for the payment of all Charges due under the Contract.

15. TERMINATION

15.1 The termination rights of the Parties set out in this Clause 15 are in addition to, and without prejudice to, any termination rights set out in the Master Services Agreement. For the avoidance of doubt, in the event of any conflict or inconsistency between the terms of the Master Services Agreement and this Service Schedule, the terms of this Service Schedule shall prevail to the extent of such conflict or inconsistency.

15.2 If the Supplier terminates this Contract due to a material breach by the Customer, or if the Customer terminates this Contract for convenience upon expiry of the Term, in each case in accordance with the Master Services Agreement, the Customer shall pay to the Supplier the Termination Sum in full (without set-off, deduction or lien).

15.3 Some technical limitations within the Services may not become apparent until after the Services have been provided for a period of time after the Actual Services Commencement Date. In such circumstances, and with the Customer's agreement, the Services may be withdrawn, in which case the Customer shall be entitled to a pro rata refund of any relevant Charges paid in advance for Services not provided. If the Customer elects to continue receiving the Services despite such technical limitations, the Customer shall be deemed to have accepted the Services as provided, and the Supplier shall have no liability for any service interruption or failure arising from those technical limitations.

15.4 When returning Goods to the Supplier pursuant to the Contract, the Customer must remove any security and other protective features that prevent the Supplier from accessing such Goods.

15.5 On termination of the Contract for any reason:

(a) the Customer shall immediately cease all use of the Services and/or the Documentation;

(b) any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Contract which existed at or before the date of termination shall not be affected or prejudiced; and

(c) where applicable, the Customer shall return to the Supplier or, at the Supplier's request, irrevocably delete and destroy any copies of or object code related to Surgery Intellect in the Customer's possession or control, and certify in writing to the Supplier that this has been done.

16. PROPRIETARY RIGHTS

16.1 The Customer acknowledges and agrees that the Supplier and/or its licensors own all Intellectual Property Rights in Surgery Intellect, the Goods (excluding Customer Equipment), Services, Software and the Documentation. Except as expressly stated herein, this Contract does not grant

the Customer any rights to, under or in, any Intellectual Property Rights or any other rights or licences in respect of or arising from Surgery Intellect, the Services, Software and/or the Documentation.

16.2 The Supplier confirms that it has all the rights in relation to the Goods, Services and the Documentation that are necessary to grant all the rights it purports to grant under, and in accordance with, the terms of the Contract.

16.3 The Customer shall own all right, title and interest in and to all of the Customer Input that is not personal data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of all such Customer Input.

16.4 The Customer grants the Supplier a perpetual, non-exclusive, worldwide, royalty-free and sublicensable right to use, copy, store, disclose, transmit, transfer, publicly display, modify and create derivative works from Customer Input and Customer Usage Data only as necessary to:

(a) Provide the Goods, Services, Documentation and Support Services;

(b) collect and use data derived from the Customer's use of the Service, including but not limited to interaction logs, feature usage, and performance metrics, for the purposes of analytics, service improvement, and platform optimisation;

(c) create and compile aggregated and/or anonymised data sets;

(d) otherwise in accordance with applicable laws;

(e) train, develop, and improve the Service (including any part thereof such as Surgery Intellect); and/or

(f) as agreed between the parties in writing.

16.5 For the avoidance of doubt:

(a) the Supplier's use of the Customer Input and Customer Usage Data as permitted under this Contract shall be in compliance withSchedule 5 (Information Governance and Data Protection); and

(b) the Supplier and/or its licensors may continue to use any improvements, learnings, or enhancements to Surgery Intellect and/or the Services derived from Customer Input and Customer Usage Data, provided that the Customer Input and Customer Usage Data itself is not disclosed or used in a manner that identifies the Customer or any individual.

(c) the Supplier may create and use aggregated and/or anonymised data derived from Customer Usage Data for any lawful purpose, provided such data does not identify the Customer or any individual.

16.6 The Supplier and/or its licensors own all Intellectual Property Rights in Surgery Intellect Output (excluding Customer Input), which shall vest in the Supplier and/or its licensors upon creation of

such Surgery Intellect Output and the Supplier hereby grants the Customer, for the duration of the Contract, a non-exclusive, non-transferable, revocable and non-sublicensable licence to use, copy and modify Surgery Intellect Output in the course of its patient care practice.

16.7 The Customer acknowledges and accepts that certain Surgery Intellect Output may not be intelligible, interpretable or capable of effective use unless used within the Software or in connection with the Service. Accordingly, the Supplier shall have no liability for any loss, error, or inaccuracy arising from use of Surgery Intellect Output independently of the Software or Services.

17. THIRD PARTY PROVIDERS

17.1 The Customer acknowledges that the Services may enable or assist it to access the website content of, correspond with, and purchase products and services from, third parties via third-party websites and that it does so solely at its own risk. The Supplier makes no representation, warranty or commitment and shall have no liability or obligation whatsoever in relation to the content or use of, or correspondence with, any such third-party website, or any transactions completed, and any contract entered into by the Customer, with any such third party. Any contract entered into and any transaction completed via any third-party website is between the Customer and the relevant third party, and not the Supplier. The Supplier recommends that the Customer refers to the third party's website terms and conditions and privacy policy prior to using the relevant third-party website. The Supplier does not endorse or approve any third-party website nor the content of any of the third-party website made available via the Services.

18. INDEMNITY

18.1 The Customer shall defend, indemnify and hold harmless the Supplier against claims, actions, proceedings, losses, damages, expenses and costs (including without limitation court costs and reasonable legal fees) arising out of or in connection with the Customer's use of the Goods, Services, Documentation and/or Surgery Intellect Output, provided that:

(a) the Customer is given prompt notice of any such claim;

(b) the Supplier provides reasonable co-operation to the Customer in the defence and settlement of such claim, at the Customer's expense; and

(c) the Customer is given sole authority to defend or settle the claim.

18.2 The Supplier shall defend the Customer, its officers, directors and employees against any claim that the Customer's use of the Goods, Services or Documentation in accordance with this Contract infringes any third party Intellectual Property Rights, and shall indemnify the Customer for any amounts awarded against the Customer in judgment or settlement of such claims, provided that:

(a) the Supplier is given prompt notice of any such claim;

(b) the Customer does not make any admission, or otherwise attempt to compromise or settle the claim and provides reasonable co-operation to the Supplier in the defence and settlement of such claim, at the Supplier's expense; and

(c) the Supplier is given sole authority to defend or settle the claim.

18.3 In the defence or settlement of any claim pursuant to clause 18.2, the Supplier may procure the right for the Customer to continue using the Services, replace or modify the Services so that they become non-infringing or, if such remedies are not reasonably available, terminate this Contract on 2 Business Days' notice to the Customer without any additional liability or obligation to pay liquidated damages or other additional costs to the Customer.

18.4 In no event shall the Supplier, its employees, agents, suppliers and sub-contractors be liable to the Customer to the extent that the alleged infringement is based on:

(a) a modification of the Goods, Services or Documentation by anyone other than the Supplier; or

(b) the Customer's use of the Goods, Services or Documentation in a manner contrary to the instructions given to the Customer by the Supplier; or

(c) the Customer's use of the Goods, Services or Documentation after notice of the alleged or actual infringement from the Supplier or any appropriate authority; or

(d) the Customer's or its Authorised Users' use of the Services and/or Surgery Intellect Output in combination with any products, services, or software not provided by or on behalf of the Supplier; or

(e) any modification of the Services and/or Surgery Intellect Output, by Customer or any Authorised User other than: (i) as permitted in the Contract or (ii) with the Supplier's written approval; or

(f) any use, processing, possession or control of Customer Input by (i) Customer or its Authorised Users or (ii) the Supplier in its performance of the Services or when complying with its obligations under the Contract; or

(g) With respect to Surgery Intellect Output, (i) Customer's use or creation of Surgery Intellect Output that it knew or should have known was infringing; (ii) trademark violations resulting from Customer's use of Surgery Intellect Output in trade or commerce; or (iii) Customer's disablement or circumvention of any applicable source citation, filtering, or safety tools or functions of Surgery Intellect; or

(h) the Customer's breach of this Contract.

18.5 Subject to Clause 19.4, to the extent that the Supplier recovers any sums from any relevant third party provider pursuant to any indemnity or equivalent contractual protection, and such sums are expressly and directly attributable to the same loss or damage suffered by the Customer in respect of the relevant claim, the Supplier shall account to the Customer for such sums. For the avoidance of doubt, the Supplier may retain any amounts recovered to the extent they relate to (a) losses or

damage suffered by the Supplier which are not the same as those suffered by the Customer, or (b) any recovery in excess of the Customer's actual loss or damage.

18.6 The foregoing and clause 19.4 state the Customer's sole and exclusive rights and remedies, and the Supplier's (including the Supplier's employees', agents', suppliers' and sub-contractors') entire obligations and liability, for infringement or alleged infringement of any third party Intellectual Property Rights by the Supplier.

19. LIMITATION OF LIABILITY

19.1 The following definitions apply in this Clause 19:

(a) **liability**: every kind of liability arising under or in connection with the Contract including but not limited to liability in contract, tort (including negligence), misrepresentation, restitution or otherwise; and

(b) **default**: any act or omission resulting in one party incurring liability to the other.

19.2 Except as expressly and specifically provided in the Contract:

(a) the Customer assumes sole responsibility for results obtained from the use of the Goods, Services and the Documentation by the Customer, and for conclusions drawn from such use. The Supplier shall have no liability for any damage caused by errors or omissions in any Surgery Intellect Output or any Customer Input, information, instructions or scripts provided to the Supplier by the Customer in connection with the Services, or any actions taken by the Supplier at the Customer's direction;

(b) all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from the Contract; and

(c) the Goods, Services and the Documentation are provided to the Customer on an "as is" basis.

19.3 Nothing in the Contract excludes the liability of the Supplier:

(a) for death or personal injury caused by the Supplier's negligence;

(b) for fraud or fraudulent misrepresentation; or

(c) for any other liability which cannot be excluded or limited by applicable law.

19.4 Subject to clause 19.2 and clause 19.3:

(a) the Supplier shall have no liability for any:

(i) loss of profits,

(ii) loss of business,

(iii) wasted expenditure,

(iv) depletion of goodwill and/or similar losses,

(v) loss or corruption of data or information,

(vi) the Customers use of Surgery Intellect Output in the ordinary course of its patient care practice, including without limitation any circumstances arising out of the sale and/or supply (or both) of the Customer's medical services to patients or otherwise, whether or not such medical services were based on, or informed by, Surgery Intellect Output (in whole or in part).

(vii) any special, indirect or consequential loss, costs, damages, charges or expenses; and

(b) the Supplier's total aggregate liability to the Customer (including in respect of the indemnity at Clause 18.2), in respect of all defaults shall not exceed the Cap. Where a single claim, or a series of connected claims, arises from defaults occurring in more than one Contract Year, the Supplier's total liability in respect of such claim(s) shall not exceed the Cap applicable in the Contract Year in which the claim is first made.

(c) in Clause 19.4(b), the cap is the total Charges payable by the Customer within the Contract Year in which the defaults occurred (**Cap**).

19.5 Subject to Clause 19.3, the Supplier shall not be liable for any acts or omissions of any subcontractor or third-party provider engaged in connection with the Services, including (without limitation) providers of connectivity, telecommunications or network services. Any failure or delay arising from such acts or omissions shall not constitute a breach of this Agreement.

19.6 Nothing in the Contract excludes the liability of the Customer for any breach, infringement or misappropriation of the Supplier's Intellectual Property Rights.

19.7 This Clause19 shall survive termination or expiry of the Contract howsoever arising.

20. Conflict

If there is an inconsistency between any of the provisions in the main body of this Service Schedule and the Schedules, the provisions in the main body of this Service Schedule prevail.

21. Assignment

21.1 The Customer shall not, without the prior written consent of the Supplier, assign, transfer, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any of its rights and obligations under the Contract

21.2 The Supplier may at any time assign, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any or all of its rights and obligations under the Contract.

22. Governing law and jurisdiction

22.1 The Contract and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and interpreted in accordance with the law of England and Wales.

22.2 Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with the Contractor its subject matter or formation (including non-contractual disputes or claims).

SCHEDULE 1
SPECIFICATION

Annex A – Surgery Intellect Features and Functionality

Feature	Description of feature	Example scenario
Capture of face to face and telephone consultations	Continuously and passively listens to conversations between patients and clinicians	A clinician begins a consultation with a patient. The Software is activated and continuously listens in the background, capturing the entire conversation as the consultation progresses.
Speech to text transcription	Converts spoken dialogue into structured, text format	As the clinician and patient speak, the Software captures the conversation generating a transcription that is displayed as soon as the consultation is concluded. As the clinician dictates for clinical and non-clinical administrative tasks they are captured and made available for workflow use.
Clinical summarisation	Extracts key clinical elements and condenses full transcription into a concise note	After the consultation, the Software generates a concise clinical note summarising the key points (e.g., symptoms, diagnosis, treatment plan) from the full transcription for the clinician to review.
Suggested structured coding	Identify and tag UK-standard SNOMED CT codes or other structured data from the conversation	The Software identifies clinical terms during transcription and tags them with SNOMED CT codes (e.g., “Type 2 Diabetes” → SNOMED code 44054006) for structured data capture.
Referral identification	Detect clinicians’ suggested action to onward refer during consultation	The Software detects this intent by the clinician to make a referral and flags that a referral is required. For example, when during the

		consultation, the clinician says, “I’ll refer you to a cardiologist.”.
Referral summarisation	Generate a concise, referral-appropriate summary for clinician review	The Software generates a concise summary specifically tailored for the referral letter, highlighting the reason for referral, key clinical findings, and relevant history.
Automated referral template population	Auto-populate referral letter with intelligent summarisation for referral	The Software pre-fills a referral form with relevant patient details, clinical notes, and structured data. The clinician reviews and validates the information before submission.
Patient summarisation	Generate a concise, patient-appropriate summary for clinician review	The Software generates a concise summary specifically tailored for the patient letter, summarising the patient consultation and any onward actions.
Automated patient template population	Auto-populate patient letter with intelligent summarisation for patient	The Software pre-fills a patient letter with relevant patient details, clinical notes, and structured data. The clinician reviews and validates the information before submission.
Guardrails against misuse	Prevent end users from generating content that is beyond intended use	The Software does not have the ability for a clinician to attempt to get advice or produce inappropriate output which is beyond the intended use of transcription, summarisation and coding of the consultation.
Clinician review and approval of generated content	Allow clinicians to review / edit the generated transcription and / or summarisation and approve or reject parts of the text	The clinician can open the generated output(s) edit any inaccuracies, remove or reject elements, correct any omissions and approve the suggested input to the patient record.
Integration with EPRs – EMIS, TPP SystemOne and Medicus	Seamlessly commit the clinicians’ approved output into their clinical	Once approved, the note is automatically committed to the patient’s record in the NHS Electronic Patient Record (EPR) system using secure, approved integration methods. The

	record of the identified patient	Software ensures the correct patient record is updated by relying on the unique patient identifier.
Visibility of solution performance	The provision of dashboards / reporting for users to view and understand how the Software is performing.	Reports are available in the Reports Console on usage and the Tortus Shell provides information on accuracy.

This specification meets that required by NHS England for the provision of ambient voice technology for the transcription, summarisation and suggested coding of a clinical consultation.

Annex B - NavBar Features and Functionality

The Software is incorporated in the Suppliers softphone functionality normally incorporated in its Surgery Connect product. Customers who do not have Surgery Connect will access the Services via the NavBar which has the following telephony and video call features and functionality, in addition to those detailed above:

Feature	**Functions available**
Active Patient	Outbound Call
	SMS
	Send Photo Request
	Video Call
	View patient contact history
	File patient communications from patient contact history
Appointment List	View appointment list by session holder name
	View appointment list by session name
	View appointment - filter by site name*
	View appointment filter by clinic type*
	View appointment filter by slot type*
	Appointment - view more than 90 days in advance
	Appointment - Status
	Appointment - view Slot notes
	File patient communications from patient contact history
	Bulk SMS from Appointment list
	Patient contact call
	Patient contact SMS
	Patient contact send photo request
	Patient contact video call
	Patient contact view contact history

Call controls	Copy inbound number to clipboard
	Answer audio call
	Answer video call
	Pause Recording
	Transfer call
	Place caller on hold
	Mute
Communications Window	Photo requests sent
	Photos received
	Call History
	3rd Party Conferencing
Contacts	Colleagues
	Directory
	View directory contact notes
	View Colleague contact notes
	Remember preferred Directory view
	Favourite Directory Contacts
Contact History User (Call History)	View available contacts
	Click to call
	Call icons
	Access to own call recordings
Device Management	Select Softphone
	Latency Indicator
Settings	Version number
	Check for updates

	Microphone
	Camera
	Secondary ringer
	Select Monitor to display
	Ringtone Selection
	Contacts
	Launches Diagnostics Window
	Quick close
	Access Help guides
	Quick File Telephone Calls
	File SMS by default
	Display to show NavBar
	Hides Phonebar
	Call History
	Contacts
	Device Manager
	User Status
	Communications
	Auto login device preference
	Auto Login device preference
	List of keyboard shortcuts
	Change User Status

SCHEDULE 2
HELP DESK SERVICE LEVELS

Operational Hours for the Support team are between 8.00am and 5.30pm Monday to Friday, excluding public and bank holidays. All other hours are classed as being outside Business Hours.

The Supplier shall prioritise all Faults based on its reasonable assessment of the severity of the Fault reported by the Customer and respond to all support requests in accordance with the response times specified in the table set out below.

Agreement level: Gold	
Minor Problems	Report via the X-on Support Portal or report by phone 0333 332 6633, in Business Hours. **Time to respond - 4 Business Hours.** **Time to investigate and address Faults - 8 Business Hours**
Serious Problems	Report via the X-on Support Portal or report by phone 0333 332 6633, in Business Hours. **Time to respond - 1 working hour** **Time to investigate and address Faults - 4 Business Hours**
Critical Problems	Report via the X-on Support Portal and then follow up by phone, quoting the ticket number, to 0333 332 6633, in Business Hours. Report by phone to duty engineer on 0333 555 8 999 at all other times. **Time to respond - 15 minutes.** **Time to investigate and address Faults - 1 working hour.**
Assistance with Self-serve Configuration Changes	Available by phone 0333 332 6633 in Business Hours. Subject to service level general terms and conditions.
Service Availability	99.9% availability
Escalation Path	If not satisfied by the response provided by the Support Team, escalate in the first instance to the Support Team Leaders on 0333 111 0000.

	Within Operational Hours contact the Support Team Leaders by email to supportteamleaders@x-on.co.uk
Further Escalation Path	If not satisfied by the response provided by the Support Team Leaders, escalate by email stating ticket number(s) to: a. Head of Technical Services: chris.finbow@x-on.co.uk b. Operations Director gary.bishop@x-on.co.uk

1. SUPPORT SERVICES

1.1 The Service Levels set out above are target times only and do not constitute performance guarantees. Failure by the Supplier to meet any Service Level shall not constitute a breach of the Contract, nor shall it entitle the Customer to terminate the Contract, withhold payment for Services provided, or claim any form of compensation, unless expressly agreed otherwise in writing.

1.2 There may be circumstances where restoration or resolution of a Fault is delayed due to third-party dependencies (being circumstances beyond the Supplier's reasonable control, including but not limited to delays caused by third-party suppliers or the provision of defective or incompatible goods or services by such suppliers). In such circumstances, the Supplier shall not be liable for any resulting delay, impact, or failure suffered by the Customer.

1.3 The Supplier reserves the right to reclassify the priority level of any reported issue following initial assessment or upon implementation of a temporary workaround.

1.4 The Customer acknowledges that the Supplier's ability to meet the Service Levels is dependent on the Customer providing timely access, information, and cooperation. The Supplier shall not be liable for any delay or failure to meet the Service Levels where such delay or failure is attributable to the Supplier's failure to provide reasonable assistance, access, or communication.

2. CUSTOMER REPORTING

To assist the Supplier in meeting the service levels under this Schedule 2, when reporting an issue, the Customer shall provide the Supplier with:

i. the date and time at which the problem occurred;

ii. the Services and/or Goods which the problem affected;

iii. the impact of the problem on the Services and/or Goods including a detailed description of the issue, including (but not limited to):

iv. the components involved, and

v. the Activity ID involved in the issue;

vi. such data, documents, information, assistance and remote access to the Customer Computer System or Goods, as are reasonably necessary to assist the Supplier to reproduce operating conditions similar to those present when the Customer detected the relevant Fault and to respond to the relevant Support Request,

and any other information that the Supplier may reasonably require

3. EXAMPLES OF LEVELS OF CRITICALITY

The levels of criticality shown in the table below are examples of possible scenarios. They are not representative of actual faults which have been experienced and are not exclusive and are intended merely to give guidance as to levels of criticality.

"Inbound" calls are calls delivered to the Customer from Supplier's service platform. "Outbound" calls and SMS are communications sent from the Customer to other numbers from handsets or PCs using Supplier software.

Like all service providers, Supplier relies on other Network Providers for delivery of calls to and from an Customer, particularly BT who have a near monopoly on the “Final Mile” connection to Supplier.

Minor	**Serious**	**Critical**
Non-service affecting queries	More than 1 in 5 inbound calls fail to be processed by Supplier.	Failure of service to respond to any inbound calls.
Problems with reports and on-line real time statistical monitors.	Problems causing incorrect routing of outbound calls or SMS through Supplier.	Failure of the service to deliver any outbound calls or SMS.
Short delays in voice call service response (less than 2 seconds)	Delays in voice call service response of up to 10 seconds.	Delays to voice call service response exceeding 10 seconds.
Intermittent queries with audio quality where attributed to Supplier’s Service Delivery Platform.	Degradation of call quality affecting all calls.	Call quality problem causing complete lack of intelligibility on all calls.
Delays on administration web site.	Failure of administration web site.	.

SCHEDULE 3
IMPLEMENTATION PROCESS

Indicative Process and Schedule

The following table provides an overview of the implementation process for the Services and an indicative timetable for an existing Surgery Connect customer. Annex A contains the additional implementation steps for non-Surgery Connect customers using NavBar.

Stage	Activity	Timeline
Contract Signed	Contract completion and HubSpot notification issued	Day 0
Service Activation	Toolbox values configured and feature enabled	Within 2 business days
Welcome & Onboarding	Welcome email, onboarding pack, and support booking link issued	Within 2 business days
Phonebar Updates	Practice completes Phonebar upgrades to v8.3.3+	Prior to go-live
Go-Live	Surgery Intellect activated and available to users	Agreed go-live date
Pulse Survey	Early experience feedback survey issued	2 weeks post go-live
Success Review	Customer Success follow-up/check-in call	1 month post go-live

Supplier Responsibilities

- Confirmation of contract completion
- Internal notification to Customer Success and Accounts teams
- Central activation of Surgery Intellect within the Toolbox
- Validation that all users are running Phonebar version 8.3.3 or above
- Configuration of required Toolbox values at Service and User level

1) **Customer Onboarding**
   a) Welcome email issued by the Customer Success Team

b) Onboarding pack provided, including:
   i) Deployment guidance
   ii) Phonebar update instructions
   iii) User guidance documentation

c) Optional 30-minute onboarding support session with a Customer Success Advisor

2) **Go-Live Support**
   a) Support provided during deployment and activation
   b) Assistance with Phonebar upgrades where required
   c) Optional Training 30 minute - Guidance on enabling users and accessing the feature

3) **Post Go-Live Adoption**
   a) Pulse survey issued two weeks after go-live to gather feedback and identify support needs
   b) One-month check-in call with Customer Success to review adoption, progress, and any outstanding actions

Customer Responsibilities

The following activities remain the responsibility of the customer:

- Completing all required DCB0160 compliance or internal governance processes in order to understand the clinical risk of the Technical Limitations inherent within the Software
- Managing any local operational or policy decisions relating to call recording and usage
- Ensuring all users update to the required Phonebar version
- Supporting users with clinical system login credentials
- Ensuring local device, network, and clinical system readiness
- Reviewing and completing recommended Academy training courses (optional)

Annex A - NavBar Implementation

The following additional implementation processes are required for NavBar:

Indicative Process and Schedule

The following table provides an overview of the implementation process for the Services and an indicative timetable for an existing Surgery Connect customer. Annex A contains the additional implementation steps for non-Surgery Connect customers using NavBar.

Stage	Activity	Timeline
Contract Signed	Contract completed and HubSpot onboarding triggered	Day 0
Service Setup	Service created and configuration values applied	Within 1–2 business days
User Preparation	User information gathered and SSO access configured	Within 2–5 business days
Welcome & Onboarding	Welcome email, onboarding documentation, and training resources issued	Within 5 business days
Phonebar Updates	Customer updates all users to Phonebar version 8.3.3+	Prior to go-live
Training	Optional onboarding and Lunch & Learn sessions delivered	Prior to or shortly after go-live
Go-Live	NavBar activated and available to users	Agreed go-live date
Post Go-Live Support	Ongoing Customer Success and Support Portal assistance	Ongoing

Additional Supplier Responsibilities

- Confirmation of contract completion
- Internal notification to Customer Success and Accounts teams
- Central activation of Surgery Intellect within the Toolbox
- Validation that all users are running Phonebar version 8.3.3 or above
- Configuration of required Toolbox values at Service and User level

1) Installation and Set Up

a) Create the service as a dedicated Non-Surgery Connect account
b) Configure all required account values, permissions, and service restrictions
c) Enable NavBar functionality centrally
d) Configure user permissions and standard user access

e) Create initial user accounts and SSO access
f) Configure withheld CLI settings and required service values
g) Configure the inbound number required for 999 emergency call routing
h) Upload the initial colleague directory
i) Enable call recording and standard retention policies
j) Support customers with Phonebar updates and activation steps
k) Provide onboarding guidance and deployment documentation

2) Customer Onboarding

a) The onboarding process is initiated automatically through HubSpot workflows
b) Customer Success will issue a welcome email and onboarding documentation
c) Customers can book onboarding support sessions with the Customer Success Team
d) Customers will have access to:
    i) Academy training resources
    ii) Getting Started with Phonebar training
    iii) Lunch & Learn training sessions
    iv) Support documentation and Help Centre guidance
e) A 20-minute NavBar training session is also available to support adoption and onboarding

3) Go-Live Support

a) Support provided during deployment and activation

4) Post Go-Live Adoption

a) Customer Success will provide ongoing onboarding support
b) Customers can raise queries through the Support Portal
c) Additional user setup or configuration requests can be managed through the Customer Success Team
d) Pulse surveys and follow-up reviews may be conducted to support adoption and ongoing success

Additional Customer Responsibilities

- Providing user lists, names, roles and email addresses for setup

SCHEDULE 4
QUALITY STANDARDS

Annex A – Key standards

Clinical Safety Requirements:

- Surgery Intellect powered by TORTUS is a UKCA Class 1 Medical Device
- DCB0129 Compliant
- DTAC ready

Cyber Security Requirements:

- Cyber Essentials Plus certified
- ISO 27001 Information Security Management Systems accredited
- DSPT Ready Status

NHS England AVT Registry:

Surgery Intellect powered by TORTUS has provided all the necessary evidence to NHS England to be listed on the Ambient Voice Technology Self-Certified Supplier Registry.

Annex B - Other standards:

- ISO 9001 Quality Systems accredited
- ISO 14001 Environmental Management Systems accredited
- ISO 22301 Business Continuity Management accredited
- ISO 42001 Artificial Intelligence Management Systems accredited

SCHEDULE 5
INFORMATION GOVERNANCE AND DATA PROTECTION

Recitals:

(1) This Contract requires the Supplier to process Personal Data ("Processor") on behalf of the Customer (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 Contract 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 Customer and the Supplier undertake to comply with the provisions of this Schedule in the performance of their Contract.

(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 Contract;
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 Customer 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 Customer 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 Customer 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 Customer'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 Customer 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 Customer's Confidential Information, and any other information provided to the Supplier by the Customer in relation to this Schedule and/or the Contract, 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 Contract. 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 Customer's written discretion, destroyed securely or returned to the Customer when it is no longer required. The Supplier shall not, and shall ensure that the staff do not, use any of the Customer's Confidential Information received otherwise than for the purposes of performing the Supplier's obligations in this Schedule and the Contract.

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 Customer (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 Customer 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 Contract 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 Customer 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 Customer'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 Customer and shall provide full information as may be reasonably requested by the Customer 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 Contract, the Parties shall comply with the Data Protection Protocol in respect of such matters.

3.3 The Supplier and the Customer 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 Customer 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 Contract;

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 Customer 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 Contract, the Supplier shall indemnify and keep the Customer 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 Customer 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.

For further background on the technical architecture, data flows, or security measures 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 Customer to transcribe, summarise and code conversations between the Customer's staff and patients.
Duration of the Processing	For the duration of the Contract between the Supplier and the Customer.
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 Customer; clinicians and authorised Customer 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 Contract, 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 Instructions

(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 Contract. 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 Contract). 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 Contract, 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 Personal Data Breach concerning data Processed by the Controller

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 Contract 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 Contract 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 Contract 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 Contract 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 Contract, 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