Accurx Terms & Conditions for G-Cloud 15

Accurx Scribe

Accurx Scribe: the integrated ambient voice technology solution for all NHS organisations

September 2026 | Version 1.0

Table of Contents

Supplier Acceptable Use Policy

Unless defined within this Supplier AUP, all capitalised terms in this Supplier AUP shall have the meaning set out in Joint Schedule 1 (Definitions), except where otherwise stated or the context otherwise requires; and

In order to keep the Platform (as defined in the Supplier Licence Terms) running in a safe, secure and uninterrupted way, the Supplier requires the Service Recipients and all Authorised Users (both as defined in the Supplier Licence Terms) to agree not to misuse it. The Buyer agrees that it has, and shall procure that any Buyer Users and all Authorised Users agree that they have, understood this Supplier AUP and in doing so agree:

1. that they have understood and agree to the Product Disclaimers (as set out and defined in the Supplier Licence Terms);
2. not to use profanities or expletives or send abusive messages while using the Platform;
3. not to use the Platform for communications in an emergency;
4. not to use the Platform for any purpose that is unlawful under any applicable law or prohibited by this Supplier AUP;
5. not to use the Platform to commit any act of fraud or to publish falsehoods, misrepresentations or misleading statements;
6. not to use the Platform for the purposes of promoting unsolicited advertising or sending spam;
7. not to use the Platform to simulate communications from the Supplier or another service or entity in order to collect identity information, authentication credentials, or other information ("phishing") or to impersonate someone;
8. not to use the Platform to gain unauthorised access to or use of computers, data, systems, accounts or networks;
9. to abide by the NHS England End User Organisation Acceptable Use Policy for use of NHS England Services that transact Personal Data (**NHS England EUO AUP**), a copy of which is attached at Annex A of this Supplier AUP, to the extent the Platform is being used in jurisdictions and with integrations or services that are covered by NHS England guidance and obligations;
10. not to distribute any material while using the Platform that is unlawful, harmful, infringing, offensive, discriminatory, or which facilitates any illegal activity or depicts

sexually explicit images or content that may cause damage or injury to any person or property;

11. to follow any internal protocols or procedures set by their organisation which relate to use of the Platform;
12. to check and use the Platform regularly to ensure no communications or actions are missed and to ensure continuation of care;
13. to use the Platform only in a professional way in connection with the provision of direct care to patients including only communicating with patients or other healthcare professionals in relation to this care (i.e. do not use the Platform for casual, social communications with friends);
14. to safeguard access to their devices that are used to access the Platform;
15. to configure their devices and your internet connection correctly in order to access the Platform and use their own virus protection software;
16. to maintain a secure and confidential password for their use of the Platform and not to attempt to circumvent password or user authentication methods;
17. not to share their unique login credentials with anyone else;
18. to use a NHS approved domain name for their login email address when creating an Account (as defined in the Supplier Licence Terms), such as nhs.net or nhs.uk, as these are the domains that the Supplier accepts on the Platform in accordance with NHS England's secure email standard (DCB1596);
19. to inform the Supplier immediately if they suspect any unauthorised access to their account on the Platform;
20. to be responsible for all actions in their Account on the Platform;
21. to ensure their account details are up to date, including the healthcare organisation that any Authorised User is currently employed by and, if these need updating, the Authorised User agrees to update their details by contacting support@accurx.com;
22. to always provide accurate and complete information and to be responsible for all data they provide directly or indirectly via the Platform (such as the content of messages and questionnaires) and any data derived from their use of the Platform;
23. not to do anything that infringes, misappropriates or violates the Supplier or any third-party's Intellectual Property Rights or other rights (such as privacy, publicity and other proprietary rights);
24. not to use the Platform for any commercial or financial gain;
25. not to use the Platform in a way that could damage, disable, overburden, or

compromise in any way the confidentiality, integrity or availability of the Supplier's systems or interfere with other users;

26. not to attempt to copy, modify, duplicate, create derivative works from, or otherwise change the whole or any part of the Platform or attempt to decompile, disassemble or reverse engineer the Platform;

27. not to attempt to access all or any part of the Platform in order to build a product which competes with the Platform; and

28. to use individual email addresses when creating an Account and to not create an Account using generic or team email addresses (e.g. musculoskeletal@trust.nhs.net or info@gppractice.nhs.net).

The Supplier's obligations and rights under this Supplier AUP

In order to identify any breaches of this Supplier AUP, the Supplier will monitor the use and content of messages sent on the Platform for safeguarding purposes. The Supplier may also monitor the Platform for usage rates and to check whether messages have been read and/or actioned. In the event a message has not been read or actioned in a timely manner the Supplier may contact the Authorised User and check whether access to the Platform is still required. These monitoring and processing activities are covered by the Supplier Data Processing Agreement.

Without prejudice to any other rights or remedies available to the Supplier, if the Supplier knows or has reasonable grounds to suspect that any Buyer User or Authorised User is acting in breach of its obligations under this Supplier AUP, the Supplier may permanently or temporarily suspend or disable the relevant Service Recipient's or Authorised User's Account or access to the Platform in accordance with Framework Special Term 7 if the Supplier considers that the conditions in Framework Special Term 7 have been met as a result of such breach. In addition to any requirements of the Contract, the Supplier may also report any contraventions of this Supplier AUP to the relevant Service Recipient(s) and/or any other organisation by which the Authorised User is employed or through whom the Authorised User has gained access to the Platform.

ANNEX A: NHS ENGLAND EUP AUP

End User Organisation Acceptable Use Policy for use of NHS England Services which transact Personal Data

The Connecting Party has signed a Connection Agreement with NHS England. The Connecting Party's products or services integrate or make use of Service(s) provided by NHS England. This End User Organisation AUP has been drafted to support the provision of the Connecting Party's products and services to the End User Organisation in relation to the integration or use of Service(s).

NHS England recognises that there could be many arrangements in relation to different products and services provided by the Connecting Party and their delivery of, access to and receipt of NHS data.

It is recognised that:

1. not all Connecting Parties will have End User Organisations associated with all Services;
2. in some circumstances a lead public sector End User Organisation will be authorised to act for a number of End User Organisations, and takes responsibility for disseminating the obligations set out in this End User Organisation AUP to the other End User Organisations and individuals within them; and
3. the Connecting Party's products or services may be delivered by the Connecting Party directly to Individual End Users.

STATUS

- This End User Organisation AUP shall govern connection to and use of the Services by all End User Organisation(s).

End User Organisation Obligations:

- End User Organisations shall only share data in accordance with the law and applicable DHSC, government and regulators' guidance and policies.
- End User Organisations cannot receive data unless they are and remain fully registered with the Data Security and Protection Toolkit (https://www.dsptoolkit.nhs.uk/) and have a current latest status rating of at least 'standards met' or (where applicable) of 'approaching standards'.
- End User Organisations are responsible for (together with any End User Organisation which is the public sector commissioning entity where relevant): choosing the Connecting Party's products and services; ensuring that the Connecting Party's products and services meet its requirements and are secure, clinically safe and legally

compliant; ensuring that the Connecting Party provides updates to and maintains its products and services, provides helpdesk and incident management services and shares any incidents impacting Services with NHS England; all arrangements with the Connecting Party for the testing, local assurance, acceptance and deployment to the End User Organisation of the Connecting Party's products and services; onboarding, service management and delivery of the Connecting Party's products and services to Individual End Users.

- End User Organisations are responsible for compliance with DCB0160 (as updated), including but not limited to management of clinical risk including establishment of a framework within which the clinical risks associated with the deployment and implementation of a new or modified health IT system are managed, its local Hazard Log, management of risks transferred by the Connecting Party and implementation of appropriate mitigation actions and controls.

- NHS England may ask the Connecting Party to provide contact information and summary information in relation to its End User Organisations. For example, to understand users of the Services and in circumstances where there is a service interruption, or a data breach, or a clinical risk issue associated with the data. End User Organisations must co-operate in the provision of such information on request from the Connecting Party.

- End User Organisations shall use the Service(s) in a manner that is consistent and compliant with this End User Organisation AUP. The End User Organisation shall ensure that the content of this End User Organisation AUP is disseminated to all staff, employees or contractors and shall incorporate it into training (where relevant).

- End User Organisations shall not include any terms in its arrangements with Individual End Users which conflict with the Connection Agreement or this End User Organisation AUP.

- To note, if an End User Organisation does not comply with its End User Organisation AUP, NHS England may itself, or may require the Connecting Party to disconnect the End User Organisation and/or suspend the End User Organisation's access to the Connecting Party's products or services, or otherwise, to the extent necessary to protect the Services as a whole.

- End User Organisations shall:

    - use the Services and the Connecting Party's products or services for their lawfully intended purposes only.

    - not use any of the Services and the Connecting Party's products or services in a way that could damage, disable, overburden, impair or compromise security of any system, service or product.

- co-operate with investigations and resolution of clinical safety, data protection and/or security incidents reported by the End User Organisation, an Individual End User or the relevant Connecting Party to NHS England.
- not knowingly transmit any data, send or upload any material that contains viruses, trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware.

Connecting Party Obligations:

- The Connecting Party shall only process personal data in accordance with the law and applicable DHSC, government and regulators' guidance and policies.
- The Connecting Party is fully accountable and responsible for the identification, onboarding and management of its End User Organisations (including for the service, management and delivery of its services to End User Organisations and Individual End Users), unless agreed otherwise with NHS England.
- The Connecting Party is responsible for bringing these terms to the attention of End User Organisations and Individual End Users, unless agreed otherwise with NHS England.
- NHS England is not responsible for verifying the terms of the Connecting Party's arrangements with the End User Organisations. In particular the terms and conditions governing security, information governance, clinical safety and any other applicable regulatory or compliance topics are detailed in the Connecting Party's contract with the commissioning party (which may also be the/one of the End User Organisation(s)).
- The Connecting Party shall, upon request from NHS England, provide to NHS England the identity and details of all End User Organisations associated with any Service(s) within such reasonable timescales as NHS England may request.
- The Connecting Party shall not include any terms in its arrangements with End User Organisations or Individual End Users which conflict with this End User Organisation AUP.
- The Connecting Party must provide the End User Organisation, on request, with details of the requirements, specifications, policies, guidance and documents associated with the Connection Agreement and any conformance documentation (being any information, self-assessment or other documentation used to assess or demonstrate the Connecting Party's compliance with the Connection Agreement, including the supplier conformance assessment list (SCAL), or such alternatives as NHS England may require from time to time).

NHS England's Role:

- NHS England provides access to its Services for the benefit of health and social care in England.
- NHS England has not carried out any assurance or testing of the Connecting Party's products or services as being suitable for the End User Organisation's intended use or purpose. NHS England will carry out a conformance assessment of the Connecting Party's connection method, against the requirements of the Service the End User Organisation wishes to connect to.
- NHS England shall have no responsibility for the management or enforcement of End User Organisation's / commissioning party's contract(s) for the provision of products and services by the Connecting Party.
- There are no service levels associated with the NHS England provision of Services, and there may be Service interruptions from time to time. NHS England does not provide anyone (including End User Organisations, Individual End User or the Connecting Party) with any commitment with regards to performance.
- End User Organisations understand the circumstances in which access to the Connecting Party's products and services may be altered or suspended due to the Connecting Party's failure to comply with this Connection Agreement.

UK GDPR and Data Protection Act 2018

- NHS England has a general role to support the wider NHS and the need to respect and promote the privacy of recipients of health services and of adult social care in England under the terms of the Health and Social Care Act 2012. It is generally the case that the Connecting Party is not the controller of the data received from NHS England, and rather it is the processor providing services to public sector entities. NHS England will make basic enquiries regarding the role of the Connecting Party in relation to the management of confidential and personal data. These enquiries do not replace the End User Organisation's (and any commissioning party's) role in ensuring that the End User Organisation and Connecting Party are meeting their responsibilities in law.
- The End User Organisation shall ensure it does all that is required to comply with UK GDPR and the Data Protection Act 2018, and shall conduct any data protection impact assessments required in connection with any processing in accordance with article 35 of the UK GDPR, and
    - where the End User Organisation is joint controller with the Connecting Party, in particular it remains responsible for putting in place an arrangement which complies with the requirements of article 26 of the UK GDPR,
    - where the End User Organisation is the independent controller of the data received and the Connecting Party is the processor, in particular it remains

responsible for putting in place a written contract that complies with the requirements of article 28(3) of the UK GDPR.

- The End User Organisation (together with any commissioning party) shall, and shall ensure the Connecting Party shall, abide by the Caldicott Principles, NHS Code and the NHS Constitution.
- The End User Organisation shall comply with the Data Security and Protection Toolkit (https://www.dsptoolkit.nhs.uk/), cyber security guidance and policy. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. It shall notify of incidents in accordance with Data Security and Protection Toolkit guidance and the Data Security and Protection Incident Reporting Tool. It shall cooperate with NHS England in relation to any management of a personal data breach incident.
- If the Connecting Party's products or services require identity verification of an Individual End User, the End User Organisation shall comply with DCB3051 (Identity Verification and Authentication Standard for Digital Health and Care Services) (as may be amended or replaced from time to time).

Confidentiality

- This End User Organisation AUP is not confidential, does not contain any confidential information, and may be published.

Variation

- NHS England is providing standard services and may need to make changes to the scope and delivery of those Services from time to time.
- NHS England is providing government services, and as such these may be cancelled at any time.
- NHS England may vary, replace or delete any part of this End User Organisation AUP and any of the documents referred to in it. Each varied End User Organisation AUP shall be effective from its date of publication.

Terms used in this End User Organisation AUP:

- **"Connection Agreement"** means the agreement entered into between the Connecting Party and NHS England;
- **"Connecting Party"** means the supplier of products or services;
- **"End User Organisation"** means any recipient or commissioning body using or commissioning a Connecting Party's products or services which interface with

Service(s) (whether directly, or indirectly via an agent or other commissioning body);

- **“End User Organisation AUP”** means this End User Organisation acceptable use policy;
- **"Individual End User"** means an individual recipient accessing any of the Services using the Connecting Party’s products or services which interface with Service(s) as an individual not an organisation;
- **"Service(s)"** means each of the selected products and services identified on the Services Form, which NHS England makes available and with which the Connecting Party is interfacing.

If you are an End User Organisation and have any questions about this End User Organisation AUP, please contact NHS England at: liveserviceonboarding@nhs.net.

Supplier Data Processing Agreement

Recitals

1. The Supplier has developed a software application that consists of a range of products to support healthcare organisations. The Platform (as defined in the Supplier Licence Terms) is used to communicate with and between patients, healthcare and/or social care professionals involved in the patient's care.

2. The Buyer and, where relevant, any Buyer Users are the Controllers of, and appoint the Supplier as their Processor to process Personal Data in order to provide the Services (as set out and defined in the Order Form).

3. This Supplier DPA supplements and is incorporated into the Contract between the Buyer and Supplier and regulates the provision and use of Personal Data and ensures both the Supplier and the Service Recipients (as defined in the Supplier Licence Terms) meet their obligations under the Data Protection Legislation.

4. In the event of any conflict or inconsistency between the provisions in this Supplier DPA and the remaining parts of the Supplier Terms, the provisions of this Supplier DPA shall prevail.

1. Definitions and Interpretations

1.1. The following words and phrases used in this Supplier DPA shall have the following meanings, except where otherwise stated or the context otherwise requires:

Supplier's Sub-Processor Webpage	http://support.accurx.com/en/articles/5501255-accurx-sub-processors
"Controller", "Processor", "Data Subject", "Personal Data" "processing", "process" and "Special Categories of Personal Data"	shall have the meanings given in the Data Protection Legislation;
Data Protection Legislation	means (i) the UK GDPR; (ii) the DPA 2018 to the extent that it relates to the processing of Personal Data and privacy; and (iii) any other Law in force from time to time with regards to the processing of Personal Data and privacy, which may apply to either Party in respect of its activities under this Agreement;
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss,

	alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by the Supplier and/or its sub-processors in connection with the provision of the Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems;
UK GDPR	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the UK's Data Protection Act 2018.

1.2. For the avoidance of doubt references to:

1.2.1. the "Services" (as set out in the Order Form) in this Supplier DPA shall include the Platform (as defined in the Supplier Licence Terms); and

1.2.2. "Personal Data" shall include any Personal Data contained within any Government Data and/or any Buyer Content (both as defined in the Joint Schedule 1 (Definitions)) provided to the Supplier by the Buyer and any Buyer Users under this Contract.

2. Scope

2.1. This Supplier DPA applies to all data processing activities undertaken by the Supplier on behalf of the Service Recipients.

2.2. This Supplier DPA including its Annexes constitutes the written instructions of the Service Recipients to the Supplier to process Personal Data in the manner described herein. Such instructions may be supplemented by the Service Recipients from time to time in writing.

3. Duration

3.1. This Supplier DPA shall terminate automatically once the Service Recipients and any Authorised Users that they employ no longer uses or has access to the Services. Notwithstanding the foregoing, the obligations in this Supplier DPA shall remain in full force and effect at all times when the parties are processing the Personal Data in their capacity as Data Controller and Data Processor, notwithstanding the termination of this Supplier DPA or any associated agreements.

4. Obligations of the Data Controller

4.1. The Service Recipients and the Supplier acknowledge that, for the purpose of the Data Protection Legislation, the Service Recipients retain control of the Personal Data and remain responsible for their compliance obligations under the applicable Data Protection Legislation, including but not limited to providing any required notices and obtaining any required consents, and for the processing instructions they give to the Supplier.

4.2. The Service Recipients warrant and represent that their instructions to the Supplier for the processing of Personal Data as contemplated under this Supplier DPA will comply with the Data Protection Legislation.

4.3. The Service Recipients acknowledge that they are responsible for ensuring their use of the Services to communicate with Data Subjects is appropriate and complies with Data Protection Legislation.

4.4. Annex A has been reviewed and approved by the Service Recipients and sets out:

4.4.1. the types of Personal Data and categories of Data Subject whose Personal Data are processed;

4.4.2. the categories of processing carried out under this Supplier DPA; and

4.4.3. a description of the technical and organisational measures adopted by the Supplier to protect the Personal Data.

5. Obligations of the Processor

Processing Instructions

5.1. The Supplier must only process the Personal Data to the extent, and in such a manner, as is necessary for the purpose of providing the Services and in accordance with the Service Recipients' instructions. The Supplier will not process the Personal Data in any other way or in a way that does not comply with this Supplier DPA or the Data Protection Legislation. The Supplier will notify the Service Recipients immediately if, in the Supplier's opinion, the Service Recipients' instructions infringe Data Protection Legislation.

5.2. The Supplier must comply with any instructions from the Service Recipients to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

5.3. The Supplier shall maintain the confidentiality of the Personal Data and not disclose the Personal Data to third parties, unless the Service Recipients or this Supplier DPA specifically authorise the disclosure, or as required by domestic law, court or regulator (including the Information Commissioner's Office). If a domestic law, court or regulator requires the Supplier to process or disclose the Personal Data to a third party, the Supplier must first inform the Service Recipients of such legal or regulatory requirement and give the Service Recipients an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

5.4. The Supplier must delete or return all Personal Data to the Service Recipients,

at the choice of the Service Recipients, as requested at the point of termination of this Supplier DPA and shall provide confirmation that all copies of the Personal Data have been deleted within 90 days after termination of this Supplier DPA.

Rights of the Data Subject

5.5. The Supplier must, at no additional cost to the Service Recipients, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Buyer and any Buyer Users as they may reasonably require, to enable them to comply with:

5.5.1. the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify, port and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

5.5.2. information or assessment notices served on the Service Recipients by the Information Commissioner's Office under the Data Protection Legislation.

5.6. The Supplier must notify the Service Recipients promptly in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

5.7. The Supplier must notify the Service Recipients within 5 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation. Subject to clause 5.17, if the Supplier receives a request or other correspondence from a Data Subject, and such communication relates to the Personal Data the Supplier is processing on behalf of the Service Recipients, the Supplier shall be entitled to respond to the Data Subject directly, but only to the extent necessary to assist the Data Subject in raising their response directly with the Service Recipients. The provisions of this clause requiring the Supplier to notify the Service Recipients do not apply in circumstances where the Supplier is unable to identify which Healthcare Organisation the relevant Data Subject is linked to (such as where the only information the Supplier has about that Data Subject following a communication from them is an email address or mobile phone number).

5.8. The Supplier will give the Service Recipients its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

5.9. The Supplier must not disclose the Personal Data to any Data Subject or to a third party other than in accordance with the Service Recipients' written instructions, this Supplier DPA, or as required by domestic law.

Security Measures

5.10. The Supplier must at all times implement appropriate technical and

organisational measures against unauthorised or unlawful processing, access, copying, modification, reproduction, display, or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure, or damage of Personal Data including, but not limited to, the security measures set out in Annex B of this Supplier DPA (**Security Measures**). The Supplier may modify or update the Security Measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures. The Service Recipients and the Supplier agree that the Security Measures shall constitute the Security Requirements (as defined in Joint Schedule 1 (Definitions)) required for this Contract, unless specified otherwise in the Order Form.

Compliance

5.11. The Supplier will provide reasonable and timely assistance to the Service Recipients to enable the Service Recipients to comply with their obligations under the Data Protection Legislation, taking into account the nature of the Supplier's processing and the information available to the Supplier, including in relation to Data Subjects' rights, data protection impact assessments and reporting to and consulting with the Information Commissioner's Office under the Data Protection Legislation.

5.12. The Supplier shall appoint an individual within the Supplier to act as a point of contact for any enquiries from the Service Recipients relating to the Personal Data the Supplier is processing on behalf of the Service Recipients. They can be contacted at dpo@accurx.com.

Audit

5.13. The Supplier shall, upon the Service Recipients' written request, make available such information as is reasonably necessary to demonstrate compliance with this Supplier DPA and Data Protection Legislation. Where such information is insufficient, the Service Recipients may request an audit, subject to the following conditions:

5.13.1. the audit shall relate solely to the Supplier's processing of Personal Data in connection with the Services and shall not extend to systems, facilities, personnel, or information unrelated to such processing, nor to the Supplier's commercially sensitive information;

5.13.2. except where required by a competent supervisory authority, any audit shall be conducted no more than once in any calendar year, upon at least thirty (30) days' prior written notice, during the Supplier's normal business hours, and in a manner that does not unreasonably interfere with the Supplier's business operations;

5.13.3. the audit may be carried out by the Service Recipients or a qualified independent auditor that is not a competitor of the Supplier and is subject to the Supplier's reasonable prior approval, such approval not to be unreasonably withheld or delayed;

5.13.4. the auditor shall enter into a confidentiality agreement on the

Supplier's standard terms prior to commencing the audit;

5.13.5. the Service Recipients shall bear all costs and expenses of the audit, including the Supplier's reasonable internal costs incurred in supporting the audit; and

5.13.6. the results of the audit shall be treated as Confidential Information in accordance with the Contract and used solely for the purpose of verifying compliance with this Supplier DPA.

Personal Data Breaches

5.14. The Supplier must without undue delay (and in any event within 48 hours) notify the Service Recipients if it becomes aware of a Personal Data Breach.

5.15. Where the Supplier becomes aware of a Personal Data Breach it shall, without undue delay, use its reasonable endeavours to provide the Service Recipients with the following information:

5.15.1. description of the nature of the event, including the categories of in-scope Personal Data and approximate number of Data Subjects and the Personal Data records concerned;

5.15.2. the likely consequences; and

5.15.3. a description of the measures taken or proposed to be taken to address the incident, including measures to mitigate its possible adverse effects.

5.16. If the Supplier cannot provide all the information above in the initial notification, the Supplier will provide the information to the Service Recipients as soon as it is available.

5.17. The Supplier will not inform any third party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data breach without first obtaining the Service Recipients' written consent, except when required to do so by domestic law.

5.18. The Supplier's notification of or response to a Personal Data Breach will not constitute an acknowledgment of fault or liability with respect to the Personal Data Breach. The obligations in this clause 5.18 do not apply to Personal Data Breaches that are caused by the Service Recipients or its personnel that access the Services.

The Supplier personnel

5.19. The Supplier must ensure that the Supplier personnel processing the data on the Supplier's behalf are subject to a duty of confidentiality ensuring in each case that access is strictly limited to those employees who need to access the relevant Personal Data, as strictly necessary to perform the Services in the context of that employee's duties to the Supplier, ensuring that all such employees:

5.19.1. are aware of and comply with the Supplier's duties under this Supplier DPA;

5.19.2. are informed of the confidential nature of the Personal Data and do not publish, disclose, or divulge any of the Personal Data to any third party unless directed in writing to do so by the Service Recipients or as otherwise permitted by this Supplier DPA;

5.19.3. are subject to user authentication and log on processes when accessing the Personal Data; and

5.19.4. have undertaken appropriate training in relation to Data Protection Legislation and in the use, care, protection and handling of the Personal Data.

5.20. The Supplier shall maintain up-to-date compliance with the NHS Data Security and Protection Toolkit (**DSPT**). The Supplier's published report can be found under organisation code 8JT17.

6. Sub-Processors

6.1. The Service Recipients give the Supplier a general written authorisation for the engagement of third-party sub-processors for the processing of Personal Data, subject to the terms of this Supplier DPA, Art. 32 of the UK GDPR, and the rules on transfers to third countries. The Supplier shall maintain an accurate list of its sub-processors currently on the Supplier's Sub-Processor Webpage. The Service Recipients and the Supplier agree that the Supplier's Sub-Processor Webpage shall constitute the Supplier Register of Subprocessors (as defined in the Joint Schedule 1 (Definitions)) required for this Contract.

6.2. The Supplier shall carry out due diligence on each sub-processor to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Supplier DPA. The Supplier will include terms in the contract between the Supplier and the sub-processor substantially similar to those set out in this Supplier DPA, and which are at a minimum compliant with the requirements of the Data Protection Legislation.

6.3. The Supplier will not add or change any sub-processor processing Personal Data under this Supplier DPA without first informing the Service Recipients of any intended change concerning the addition or replacement of other processors by updating the Supplier's Sub-Processor Webpage at least 30 days in advance of when a new sub-processor for the processing of Personal Data is engaged. The Service Recipients acknowledge that it is their responsibility to check regularly for any updates to the Supplier's Sub-Processors, and that the Service Recipients can choose to receive email updates by following the instructions on the Supplier's Sub-Processor Webpage.

6.4. The Service Recipients has the right to object to the processing of Personal Data by a new sub-processor on reasonable and explained grounds by providing a written objection to privacy@accurx.com within 10 written days

following the Supplier's notification to the Service Recipients of the intended engagement with the new sub-processor. The parties agree to use good faith efforts to resolve the Service Recipients' objection. Where an objection cannot be reconciled with the Service concept or technological requirements of the Supplier, either party may terminate the applicable features of the Service with immediate effect.

6.5. Where the sub-processor fails to fulfil its obligations under the written agreement with the Supplier which contains terms substantially the same as those set out in this Supplier DPA, the Supplier remains fully liable to the Service Recipients for the sub-processor's performance of its agreement obligations.

Cross-border Transfers

6.6. The Service Recipients consents to the Supplier processing Personal Data outside the UK and/or the EEA provided that:

6.6.1. the Supplier is processing the Personal Data in a territory which is subject to adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. The Supplier shall identify on the Supplier's Sub-Processor Webpage the territory that is subject to such adequacy regulations; or

6.6.2. the Supplier participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Supplier (and, where appropriate, the Service Recipients) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR. The Supplier shall identify on the Supplier's Sub-Processor Webpage the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Supplier must promptly inform the Service Recipients of any change to that status; or

6.6.3. the transfer otherwise complies with the Data Protection Legislation.

7. Authority to agree to the terms of this Supplier DPA

7.1. If the Buyer entering into this Contract with the Supplier is an integrated care board or similar body acting on behalf of one or more Buyer Users, the Buyer represents that it is duly authorised to enter into this Contract and, in particular, is duly authorised to agree to the specific data processing terms in this Supplier DPA and any other terms of the Contract that are relevant to this Supplier DPA on behalf of the Buyer Users it represents, and shall procure that such Buyer Users will be bound by this Supplier DPA as if they were direct signatories to it.

7.2. The Buyer acknowledges and agrees that any notification requirements under this Supplier DPA shall be satisfied by the Supplier notifying the Buyer on behalf of any Buyer Users.

ANNEX A: PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. List of Parties

Data exporter(s)	
Name:	The Buyer and any Buyer Users (**Service Recipients**), as set out in the Order Form
Address:	The Buyer's address, as set out in the Order Form
Contact person's name, position and contact details:	The Buyer Authorised Representative's or Data Protection Officer's contact details, as set out in the Order Form
Role (Controller/Processor):	Controller

Data importer(s)		
Name:	Accurx Limited (**Supplier**)	
Address:	7 Curtain Rd, London EC2A 3LT	
Contact person's name, position and contact details:	*Name:*	Mischon De Reya LLP
	Role:	Data Protection Officer
	Address:	Mishcon De Reya LLP Africa House 70 Kingsway LONDON WC2B 6AH
	Email:	dpo@accurx.com
	Tel:	020 3321 7000
Role (Controller/Processor):	Processor	

2. Data Processing Description

Description	**Details**
Identity of Controller and	**Controller:** Buyer and any Buyer Users

Processor for each Category of Personal Data	**Processor:** the Supplier
Subject matter of the processing	To provide the Services (the Supplier's patient communication and engagement platform), as adopted by the Buyer and any Buyer Users from time to time.
Duration of the processing	For as long as the Buyer and, where relevant, any Buyer Users continue to use the Services.
Purposes and nature of the processing	The purposes and nature of the processing includes: • Automated solutions for recording, transcribing and summarising consultations, and generating content based on transcriptions to aid communication with and about patients. • Reviewing and validating content generated by automated solutions and the inputs to those solutions to ensure clinical safety throughout the development, monitoring and improvement of these solutions on the platform. • Healthcare and/or social care professionals may disclose patient data to the Supplier when receiving technical support and from time-to-time the Supplier's technical team may have access to patient data when they are fixing a technical issue for example via remote support, which may include screen sharing. • Security monitoring, auditing and service delivery and improvement of the Services, including creating and using Analytical Data (as defined in the Supplier Licence Terms). • Compilation of anonymised statistics about the use of the Services, such as the use of its functions by its users in communication with patients. These statistics may be used for the Supplier's own analytics and improvement purposes. The Supplier may also share these anonymised statistics publicly or with third parties. These third parties include: ○ national bodies, including Department

	of Health and Social Care and NHS England; ○ local NHS bodies, including ICBs and Primary Care Networks; and ○ partners of Accurx, including commercial organisations, charities and academic institutions.
Type of personal data	**Personal Data (relating to patients of the Data Controller):** • Patient demographic details (name; date of birth; gender) • NHS number • Mobile phone number • Email address **Personal Data (relating to healthcare and/or social care professionals):** • Name • Email address • Mobile phone number • Affiliated organisations • Job role **Sensitive Personal Data** • Content of the communications with – or regarding - patients sent via the Services (which may include patient images or documents and contain data concerning health). • Other types of data, including third party data, (which may include contents of the patient's Medical Record and data concerning health that may from time to time be required to provide the Services).
Security Measures adopted by the Supplier	As set out in Annex B
Approved Sub-Processors	As set out on the Supplier's Sub-Processor Webpage (https://support.accurx.com/en/articles/5501255-accurx-sub-processors), as updated from time to time in accordance with this Supplier DPA.

Locations at which the Supplier processes Personal Data under this Contract and international transfers and legal gateway	All Subprocessors that Process Personal Data do so in the EU, with limited exceptions outside of the EU that are subject to adequacy decisions from the EU Commission and the UK Secretary of State for the Department of Science, Innovation and Technology. The Supplier's list of approved Subprocessors is set out on the Supplier's Sub-Processor Webpage (https://support.accurx.com/en/articles/5501255-accurx-sub-processors), as updated from time to time in accordance with this Supplier DPA.
Plan for return and destruction of the data once the Processing is complete	The Supplier must delete or return all Personal Data to the Buyer and any Buyer Users, at the choice of the Buyer and any Buyer Users, as requested at the point of termination of this Call-Off Contract and shall provide confirmation that all copies of the Personal Data have been deleted within 90 days after termination of this Contract.

ANNEX B: SECURITY MEASURES

Security Measure	Detail
Measures of pseudonymisation and encryption of personal data	Personal data is stored encrypted and is protected by strong authentication and access controls on the Accurx side. For example, any databases storing personal data are secured with strict access controls limited to senior and trained staff at Accurx, and protected by Multi-factor authentication. Privileged access rights require approval and are granted on a temporary basis.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	As a cloud first company, our data is regularly backed up by our cloud services providers. We maintain a BCDR plan for the whole business and this includes measures we would take to rapidly and completely recover availability and access to the personal data in the platform. Backup restoration should take a matter of minutes once initiated.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	We regularly scan for vulnerabilities and vulnerable dependencies in our code and containers and utilise the security functionality provided by our cloud providers. We perform regular vulnerability scanning as well as undergo regular penetration tests via our cyber security partners. Tabletop incident response exercises are also undertaken in order to test our organisational security. We also have a security awareness training and internal phishing process.
Measures for user identification and authorisation	Accux account sign up and password, with admin accounts controlled by user organisations that can allow/remove accounts from the organisation. **Accurx Desktop** Permission to access clinical records through API controlled by practice management (e.g. EMIS EMAS Manager). **Accurx Web** Integration with NHS Mail and NHS.net single sign-on for Accurx Web.

Measures for the protection of data during transmission	Data is transferred using a minimum of TLS 1.2 in a secure configuration with strong cryptographic algorithms. We maintain a Cryptography & Key Management Policy which is regularly updated in line with best practice. Other transport security measures are configured such as HSTS to ensure data is transmitted over a secure connection and preload our domains where relevant.
Measures for the protection of data during storage	Physical security of our datacentres are managed by our cloud providers. The physical security of Accurx offices and devices are managed by the security and IT teams of Accurx. Measures include managed key access, CCTV, mandatory device management, and early and regular security training for staff upon joining the organisation.
Measures for ensuring events logging	We use a selection of logging capabilities to capture software and infrastructure events, to investigate technical issues, detect suspicious activity, and support Data Controllers investigating activity.
Measures for ensuring system configuration, including default configuration	Tooling provided by our cloud services providers monitor our cloud environment configuration. We utilise a modern infrastructure as code paradigm and consider relevant best practice for secure architecture, coding and deployment. Robust changes and release management processes are implemented.
Measures for internal IT and IT security governance and management	We have network security and configuration subject to strict access controls for only the IT security team. Mobile device management is a prerequisite on devices used for company business. SaaS solutions are preferred to conduct business, and access to these is centrally administered by the company's IT Teams; relevant systems are cloud-based, selected for high standards of technical and organisational security measures. Where possible, SSO (with MFA) or MFA alone is enabled.
Measures for certification/assurance of	We hold ISO27001 certification and Cyber Essentials Plus. We are required to submit an annual NHS Data Security and

processes and products	Protection Toolkit assessment.
Measures for ensuring data minimisation	Training is provided for staff about the responsibility they have in relation to IG and Security, and is designed to ensure they consider and practice data minimisation principles across the business.
Measures for ensuring data quality	Data Controllers who detect quality issues can report these through our Service Desk at support.accurx.com, and our engineers will work with them to correct the issue.
Measures for ensuring limited data retention	Unless otherwise stated, retention periods for data in the product are set in line with the Retention Policies set out in the Records Management Code of Practice. This is governed by automatic rules set in Azure or instructions issued by the data controller on retention periods in contracts/agreements or by specific communication with our service desk.
Measures for ensuring accountability	Accurx can be contacted for any data processing or security related issue through support.accurx.com. We actively maintain relevant certification and provide these to customers via our website and Trust Centre. We are registered with the ICO and list our DPO details on that page.
Measures for allowing data portability and ensuring erasure	Defined processes are in place for the provision of data in agreed formats and/or deletion of data, upon request or upon the end of contract.

Accurx Supplier Standard Terms

Supplier Licence Terms

The following Supplier Licence Terms shall govern the provision of the Platform (as defined below).

1. Definitions and Interpretation

1.1 Capitalised terms not defined herein, shall have the following meanings:

"AUP" means the Supplier Acceptable Use Policy.

"Account" means the user account that each Authorised User has to create in order to gain access to the Platform.

"Accurx Desktop" means the native application installed on an Authorised User's desktop computer that integrates with the local electronic patient record (for example EMIS or SystmOne) through which the Supplier's functionality and the Products can be accessed.

"Accurx Documentation" means those printed or online instructions, manuals, and diagrams distributed or otherwise provided by the Supplier that relate to the Platform or its use.

"Accurx Mobile" means the mobile application that allows healthcare professionals to collaborate and communicate securely.

"Accurx Scribe" means the AI enabled ambient scribe solution powered by Tandem that is available within the Platform, and is included in the definition of Product set out herein.

"Accurx Web" means the version of the Platform that is web-based and is accessible via a web browser or mobile device and does not require any software to be installed or downloaded.

"Analytical Data" means any data which is derived from the Patients', Service Recipients' and Authorised Users' use of the Platform or the Processing of Service Recipient Data, and shall include: (i) any data which is processed and stored as mathematical constructs; and (ii) statistical or aggregated data, but shall exclude any Personal Data.

"Ancillary Fees" means any costs or fees set out in the Order Form relating to additional work items (such as further implementation or training costs), and is included in the definition of Charges (as defined in Joint Schedule 1 (Definitions)).

"Authorised Use" means, as the case may be, communication with Patients in relation to the provision of direct care services in the Territory to Patients registered with the Service Recipients, or communication between healthcare professionals in the Territory.

"Authorised Users" means those healthcare professionals, employees, agents, licensees, or contractors of the Service Recipients with appropriate qualifications and expertise to provide the relevant health and care services who are authorised by the Service Recipients to use the Platform.

"BCDR Plan" has the meaning set out in clause 5.7.

"Case Study" means any case study or similar report setting out the benefits and findings of a pilot or other project undertaken by any Service Recipient and the Supplier which may be published by the Supplier (for example as an article on the Site), as defined or otherwise set out in the Order Form.

"DPA" means the Supplier Data Processing Agreement.

"Exit Plan" has the meaning set out in clause 5.6.

"Improvements" means any modifications, adaptations, developments, or any derivative works of or to the Platform or the operation of the Platform, including any Deliverables, enhancements, features, functionality, configurations, templates, documentation, or other materials that are developed as part of, or result from, any agreed improvements to the Platform under this Contract including but not limited to any new content such as information relating to proposed questions for the Supplier's questionnaire product or a message template for the Supplier's patient and/or clinician messaging product, whether derived by the Supplier from Analytical Data, made collaboratively between the Service Recipients or their Authorised Users and the Supplier, or independently by the Service Recipients or Authorised Users (including where such Improvements are created without the Supplier's prior written consent). For the avoidance of doubt, any Improvements that are incorporated into, intended to operate with, or capable of being used as part of the Platform shall constitute Improvements for the purposes of this Contract, regardless of whether such Improvements are developed for a specific Service Recipient.

"Licence Fee" means the Software-as-a-Service licence fees payable by the Buyer for access to the Platform, the Services (as set out in the Order Form) and any Deliverables (as set out in the Order Form), and is included in the definition of Charges (as defined in Joint Schedule 1 (Definitions)).

"Minimum Specifications" means the minimum requirements that the Service Recipients and their Authorised Users must ensure their devices and computers have in order for them to be able to access the Platform. The Minimum Specifications are

accessible at the following webpages, as may be updated from time to time during the Contract Period by the Supplier: a) for desktop computer requirements: https://support.accurx.com/en/articles/2317791-accurx-desktop-installation-guide-for-it-professionals; b) for web browser requirements: https://support.accurx.com/en/articles/3790180-video-which-browsers-are-supported; and c) for internet speed/connectivity requirements: https://support.accurx.com/en/articles/3223478-accurx-web-technical-requirements-for-video-consultations.

"Patient" means an individual requiring the direct care services of a Service Recipient and who are contacted by a Service Recipient in relation to their care such as via SMS, email, online consultation forms, or other electronic communication through or as part of the Platform.

"Patient Data" means information about Patients accessed by a Service Recipient using third-party services/networks/facilities such as the NHS Spine (PDS) or a clinical or medical/patient record system, as the case may be, or provided by Patients when responding to or contacting a Service Recipient and their Authorised Users via the Platform.

"Payment Terms" means the frequency at and payment method by which the Buyer agrees to pay the Supplier the Charges as set out in the Order Form.

"Platform" means Supplier's hosted or cloud-based products that are provided by the Supplier on a Software-as-a-Service basis including Accurx Desktop, Accurx Mobile, Accurx Web and any related software or ancillary products and services that are owned and provided by the Supplier and that the Service Recipients and their Authorised Users are authorised or licenced to use by the Supplier. The Platform is provided as part of the Services (as defined in Joint Schedule 1 (Definitions)).

"Product" means those products set out in the Order Form which the Service Recipients and their Authorised Users are authorised and licenced to use by the Supplier, and is included in the definition of Platform setout herein.

"Product Disclaimers" means the product-specific disclaimers set out in Annexes A and B of these Supplier Licence Terms.

"Privacy Notice" means the Supplier's privacy notice which is accessible at https://www.accurx.com/privacy-notice, as may be updated from time to time during the Contract Period by the Supplier.

"**Service Recipient"** means the Buyer and any and all Buyer Users (as defined in Joint Schedule 1 (Definitions)).

"Service Recipient Data" means the Government Data, Buyer Content and any other

data uploaded, submitted or collected via the Platform including without limitation all anonymised business data, but excluding any Analytical Data and Patient Data.

"Service Recipient Personal Data" means Personal Data contained in the Service Recipient Data which is limited to the Service Recipients' employees' names and email addresses.

"Site" means https://www.accurx.com/ and all relevant subdomains or such other URL as updated by the Supplier from time to time.

"SLA" means the Supplier Service Level Agreement as it applies to the specific Products provided to the Service Recipients and their Authorised Users under this Contract.

"Switch-on Date" means (where applicable) the date that the Service Recipients and their Authorised Users will be able to access and use the Platform. The Switch-on Date is set out in the Order Form. In the event there is no Switch-on Date specified in the Order Form, the Switch-on Date is the Start Date or the date as otherwise notified to the Service Recipients by the Supplier using any reasonable means.

"Territory" means that territory or those territories in which the Service Recipients primarily operate and provide their direct care services to their Patients or otherwise confirmed by or to the Supplier in the creation of the Account.

"Virus" means 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.

1.2 In these Terms and Conditions:

1.1.1 any words following the terms including, include, in particular for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms;

1.1.2 clause, schedule and paragraph headings shall not affect the interpretation of these Terms and Conditions;

1.1.3 unless the context otherwise requires, words in the singular shall include the plural and words in the plural shall include the singular;

1.1.4 a reference to writing or written includes e-mail;

1.1.5 references to clauses and schedules are to the clauses and schedules of these Terms and Conditions; references to paragraphs are to paragraphs of the relevant schedule to these Terms and Conditions; and

1.1.6 any capitalised words not defined within these Supplier Licence Terms shall take the meaning given to them under Joint Schedule 1 (Definitions).

2. Applicability of these Supplier Licence Terms

2.1 The Buyer and the Supplier acknowledge and agree that:

2.1.1 the Platform, Services and any Deliverables provided by the Supplier under the Contract all constitute Cloud Products as they are non-customised software which is commercially available and subject to the Supplier's standard licence terms (as set out in these Supplier Licence Terms);

2.1.2 the Supplier provides the Cloud Products on a Software-as-a-Service basis via a multi-tenant platform that is used by multiple customers;

2.1.3 the Supplier is not providing Specially Written Software or bespoke software development services under this Contract and the terms applicable to Specifically Written Software or COTS Software shall not apply to the Software provided by the Supplier to the Service Recipients hereunder; and

2.1.4 these Supplier Licence Terms set out the terms applicable to the licensing of the Platform, Services and any Deliverables and shall take precedence over any conflicting provisions in the Contract to the extent of such conflict.

3. Access to the Platform

3.1 The Buyer confirms that it and its signatory are duly authorised to enter into this Agreement on behalf of the Service Recipients and that by continuing to use and access the Platform it agrees to be bound by these Supplier Licence Terms.

3.2 The Supplier hereby grants to the Buyer:

3.2.1 a non-exclusive, non-transferable, non-sub licensable, royalty-free right to permit the Service Recipients and their Authorised Users to access and use the Platform from the Switch-on Date and during the Contract Period in accordance with these Supplier Licence Terms; and

3.2.2 a perpetual, irrevocable, royalty-free licence to permit the Service Recipients and their Authorised Users to use the Deliverables for internal business purposes only in accordance with these Supplier Licence Terms.

3.3 The licence granted in clause 3.2 shall be for the Authorised Use only and the Buyer:

3.3.1 undertakes to ensure that all Service Recipients and Authorised Users access and use the Platform in accordance with these Supplier Licence Terms and the

AUP;

3.3.2 undertakes to bring the AUP to the attention of all Service Recipients and Authorised Users; and

3.3.3 shall be responsible for all Service Recipients' and Authorised Users' breach of these Supplier Licence Terms and/or the AUP.

3.4 The Buyer shall at all times not, and shall procure that all Service Recipients and Authorised Users shall at all times not, knowingly access, store, distribute or transmit any Viruses or any material during the course of their use of the Platform that contains profanities or expletives, is unlawful, harmful, abusive, infringing, offensive, discriminatory, or which facilitates illegal activity or depicts sexually explicit images or causes damage or injury to any person or property. The Supplier reserves the right, in its sole discretion and without liability or prejudice to its other rights to the Buyer, to:

3.4.1 remove any such content (including Buyer Content and Government Data, if relevant) from the Platform;

3.4.2 suspend or disable any Buyer Users' and Authorised Users' access to the Platform in accordance with Framework Special Term 7 if the Supplier considers that the conditions in Framework Special Term 7 have been met as a result of a breach of this clause 3.4 or the AUP;

3.4.3 report any misuse of the Platform by the Authorised Users in contravention of the AUP to the relevant Service Recipient; and

3.4.4 report any evidence of serious and frequent misuse by the Service Recipients and their Authorised Users to relevant authorities and regulators as required.

3.5 Except as may be allowed by any applicable law which is incapable of exclusion by agreement between the Buyer and the Supplier, and except to the extent expressly permitted under this Agreement, the Buyer shall not, and shall procure that all Buyer Users and Authorised Users shall not, attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the software underpinning the Platform in any form or media or by any means; or attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Platform.

3.6 The Buyer shall not, and shall not attempt to:

3.6.1 access all or any part of the Platform in order to build a product or service which competes with the Platform;

3.6.2 make the Platform available to any third-party except to other Service Recipients and Authorised Users; or

3.6.3 attempt to obtain, or assist third parties in obtaining, access to the Platform, other than as provided under this clause 3.

3.7 The Buyer shall, and shall procure that other Service Recipients and all Authorised Users shall,:

3.7.1 use all reasonable endeavours to prevent any unauthorised access to, or use of, the Platform and, in the event of any such unauthorised access or use, promptly notify the Supplier;

3.7.2 keep a secure password for their use of the Platform only and that each Authorised User shall keep their password confidential and not share their login credentials with anyone else;

3.7.3 use an individual email address when creating an Account with the Supplier and not use generic or team email addresses (such as muscoskeletal@trust.nhs.net or info@gppractice.nhs.net);

3.7.4 safeguard access to their devices where they access the Platform; and

3.7.5 inform the Supplier immediately if they suspect any unauthorised access to their Account.

3.8 The rights provided under this clause 3 are granted to the Buyer only. The Buyer shall procure the other Service Recipients' and all Authorised Users' adherence to clauses 3.4 to 3.6 (inclusive of these Supplier Licence Terms. The Supplier shall not be liable for any delay, failure or breach of these Supplier Licence Terms where the Buyer does not provide such authority, information and co-operation or the Buyer fails, delays or omits to act in respect of any of its obligations under these Supplier Licence Terms.

3.9 **Accurx Scribe Fair Usage Policy:** The Service Recipients and Authorised Users acknowledge that the Supplier implements a fair usage limitation of 50 transcription consultations per Authorised User per day for Accurx Scribe to prevent system overload, ensure service quality for all users and ensure licences to Accurx Scribe are not being misused or shared between Authorised Users. Usage exceeding this limit is not possible and no further transcriptions can be made by that Authorised User for the remainder of the day. There are no concurrency limits or incremental charges associated with this Scribe Fair Usage Policy.

4. Service Recipient Data and Analytical Data

4.1 The Supplier and the Buyer shall comply, and the Buyer shall procure that the other Service Recipients comply, with their respective obligations under the Data Protection Legislation and the DPA. The Buyer and Supplier acknowledge that the Supplier:

4.1.1 will be the Processor of the Patient Data; and

4.1.2 (where applicable) will process the Service Recipient Personal Data in accordance with the Privacy Notice.

4.2 The Buyer agrees to bring the Privacy Notice to the attention of the Service Recipients and Authorised Users.

4.3 Each Service Recipient shall own all right, title and interest in and to all of its relevant Service Recipient's Data and Patient Data. The Buyer shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Service Recipients' Data and Patient Data.

4.4 The Supplier may use the Service Recipient Data during the Contract Period to create Analytical Data, which the Buyer acknowledges may be used to improve the performance and functionality of the Platform or develop Improvements.

4.5 The Supplier may track and analyse the Service Recipients' and Authorised Users' use of the Platform for the purposes of security, service delivery, auditing and to help the Supplier improve its other products and the Platform.

4.6 The Buyer and Supplier acknowledge that as the Supplier provides a Software-as-a-Service (as further described in clause 2 of these Supplier Licence Terms), clauses 17.6.1 and 17.6.3 are not relevant to the type of services provided, as such they agree that the Supplier:

4.6.1 shall only be required under this Contract to send the Buyer copies of all Government Data and any Buyer Content within 30 days of a written request from the Buyer's Authorised Representative or another appropriate individual (as confirmed in writing by the Buyer's Authorised Representative) and in a format agreed between the Supplier and the Buyer; and

4.6.2 must securely erase all Government Data and Buyer Content and any copies held by the Supplier when asked to do so by Buyer's Authorised Representative or another appropriate individual (as confirmed in writing by the Buyer's Authorised Representative).

5. Accurx's Obligations

5.1 The Supplier shall abide by and make the Platform, Service and any Deliverables available in accordance with the SLA, as relevant to the Products to which the Service Recipients and Authorised Users have access, and provide the level of user support set out in the SLA.

5.2 The Supplier shall not be liable for any breach of its obligations under clause 5.1 to the extent any non-conformance is caused by use of the Platform, Services and any Deliverables contrary to the Supplier's instructions, or any modification or alteration of

the Platform, Services and any Deliverables by any party other than the Supplier. Notwithstanding the foregoing:

5.2.1 the Buyer acknowledges and agrees that the Platform and Services will evolve over time and that functionality may be added (including any Deliverables) and removed from time to time, provided that any removals do not materially change or have a negative material impact on the Services. The Buyer and the Supplier agree that the following shall apply in relation to the Supplier's obligation to notify the Buyer of Service Modifications (as defined in clause 2.17.2 of the General Terms as incorporated by Framework Special Term 15):

5.2.1.1 The Supplier shall provide advance notice to the Buyer in accordance with clause 2.17.2(a) of the General Terms for any Service Modifications that constitute substantial changes to product functionality (such as changes that introduce novel workflows or functionality which require training and/or implementation support for Service Recipients and Authorised Users significantly in addition to the Supplier's standard training and implementation offering and services) through its product roadmap (as set out in the Order Form) or via its user support function (for example by way of a banner) or as otherwise agreed in the Order Form;

5.2.1.2 The Supplier shall not be required to provide advance notice in accordance with clause 2.17.2(a) of the General Terms for any Service Modifications that relate to the addition of any Deliverables as the Buyer agrees that these will be communicated and agreed through any Implementation Plan;

5.2.1.3 The Supplier shall not be required to provide advance notice in accordance with clause 2.17.2(a) of the General Terms for any other Service Modifications not covered by clauses 5.2.1.1 and 5.2.1.2 as these are deemed not to materially affect the Platform (for example, cosmetic and UX tweaks, bug fixes, improvements to functionality and performance optimisation);

5.2.1.4 The Supplier shall provide notice of any Urgent Service Modifications (as defined in clause 2.17.3) as agreed and set out in the Order Form; and

5.2.1.5 For the avoidance of doubt, the Supplier shall adhere to the remaining provisions of clause 2.17 of the General Terms (as incorporated by Framework Special Term 15).

5.2.2 the Supplier does not warrant that the Service Recipients' and Authorised Users' use of the Platform, Services and any Deliverables will be uninterrupted

or error-free; or that any third-party information provided, generated, obtained or otherwise accessible by the Service Recipients and Authorised Users through their use of the Platform ("**Content**") will meet the Service Recipients' requirements. All Content that is provided, generated, obtained or otherwise accessible as part of the Platform, Services and any Deliverables is provided on an "as is" basis. The Supplier assumes no responsibility for, and expressly disclaims any liability arising from use of or reliance on such Content; and

5.2.3 the Supplier shall not be in breach of the SLA to the extent any non-conformance relates to any loss in availability, delays, delivery failures, or any other loss or damage resulting from the transfer of data over third-party communications networks, services and facilities that it does not own or that are out of its control (for example the internet and any integrations such as electronic patient records and PDS), and the Buyer acknowledges that the Platform, Services and any Deliverables may be subject to limitations, delays and other problems inherent in the use of such communications facilities; and

5.2.4 the Supplier shall not be liable for any unauthorised access, use or alteration of the Service Recipients' and Authorised Users' Accounts, transmissions or content, or any Virus or malware infecting their devices as a result of the Platform, Services and any Deliverables to the extent that these arise from any use contrary to these Supplier Licence Terms and any other instructions received from the Supplier.

5.3 This 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 Contract.

5.4 Implementation

5.4.1 If requested by the Buyer in the Order Form or otherwise in writing, the Supplier shall submit to the Buyer a draft Implementation Plan within 14 (fourteen) days of the Start Date.

5.4.2 Following submission of the draft Implementation Plan, the Buyer and the Supplier shall agree and finalise the Implementation Plan within 1 (one) Month of its submission (or at a later date agreed between the Buyer and Supplier). Once agreed, the Implementation Plan shall constitute the Implementation Plan for the purposes of this Contract and will apply to any Buyer Users as well.

5.4.3 Where relevant, the Buyer and Supplier shall agree the following within the Implementation Plan:

5.4.3.1 the commencement date for access to the Platform and any Deliverables if this date differs from the Switch-on Date; and

5.4.3.2 the scope, approach and success criteria for any testing required by the Buyer for deployment of the Platform and any Deliverables as part of the implementation which shall constitute the testing procedures required by this Contract.

5.4.4 If the Buyer and Supplier are unable to agree the contents of the Implementation Plan within the time period set out in clause 5.4.2, it shall be deemed a Dispute and shall be resolved in accordance with the Dispute Resolution Procedure.

5.5 Security

5.5.1 In addition to any security requirements set out in the Framework Special Terms, the Supplier shall maintain:

5.5.1.1 an information security management system (**ISMS**) in accordance with ISO27001; and

5.5.1.2 certifications to: a) the UK Government's Cyber Essentials Plus; b) ISO27001; and c) NHS Data Security and Protection Toolkit).

5.6 Exit Management

5.6.1 The Supplier confirms that it has a template exit plan for the orderly cessation of use of the Platform, Services and any Deliverables upon termination of the Contract for any reason and that it includes:

5.6.1.1 a description of the exit process and associated timelines, including the Termination Assistance Period and the process for terminating the Service Recipients' and Authorised Users' access to the Platform;

5.6.1.2 the assistance and transition support provided by the Supplier to the Service Recipients; and

5.6.1.3 the process for access to and/or export or deletion of any Buyer Content, Personal Data and Patient Data to the Service Recipients in accordance with the DPA.

referred to as the **"Exit Plan"**.

5.6.2 The Buyer and the Supplier agree that the Exit Plan shall constitute all of the support and exit arrangements that apply to this Contract.

5.6.3 The Supplier shall provide a copy of the Exit Plan upon request from the Buyer.

5.6.4 Upon receipt of the Exit Plan, the Buyer may request reasonable updates to the Exit Plan (taking into consideration clause 2.1 and the type of services the Supplier provides) provided that such updates shall not be incorporated into the Exit Plan until they have been agreed with the Supplier (acting reasonably).

5.6.5 The Supplier may update the Exit Plan from time to time to reflect changes in the Platform, Services and any Deliverables, or operational procedures, provided that such updates do not materially reduce the Supplier's exit obligations. If the Buyer has requested and received a copy of the Exit Plan the Supplier shall:

5.6.5.1 notify the Buyer of any updates to the Exit Plan that do not materially reduce the Supplier's exit obligations; and

5.6.5.2 agree in writing with the Buyer any material amendments to the Exit Plan (such as reductions in the transition support provided).

5.7 BCDR

5.7.1 In accordance with Special Term 4, the Supplier confirms that it has a plan in place to ensure:

5.7.1.1 continuity of the Supplier's business processes and operations that support the provision of the Platform, Services and, where relevant, any Deliverables following any failure or disruption of any element of the same; and

5.7.1.2 the recovery of the Platform, Services and, where relevant, any Deliverables in the event of a Disaster.

referred to as the **"BCDR Plan"**.

5.7.2 The Parties agree that the BCDR Plan constitutes the business continuity and disaster recovery provisions for this Contract. The Supplier shall:

5.7.2.1 review the BCDR Plan at least annually to assess its suitability for the Platform, Services and any Deliverables;

5.7.2.2 test the BCDR Plan or the resilience of the Platform, Services and any Deliverables against a relevant disaster event at least annually;

5.7.2.3 update the BCDR Plan if necessary following any review or test; and

5.7.2.4 supply a copy of the current BCDR Plan to the Buyer upon request.

5.8 Notifications

5.8.1 The Buyer acknowledges and agrees that any notification requirements under these Supplier Licence Terms shall be satisfied by the Supplier notifying the Buyer on behalf of any Buyer Users.

6. Buyer's Obligations

6.1 The Buyer shall provide the Supplier with all necessary cooperation in relation to these Supplier Licence Terms and all necessary access to information as may be required by the Supplier to fulfil its obligations under these Supplier Licence Terms, including granting the Supplier full and unrestricted access to all Service Recipients' account information and activity held internally by the Supplier (for clarity this is not access to the Account) in order to allow the Supplier to undertake activities such as providing support, carrying out maintenance, reviewing analytics and data to provide insights for making improvements to the Platform and fixing any errors. The Buyer shall be responsible for setting the access rights for their Authorised Users and shall procure that any Buyer Users set the access rights for their Authorised Users and shall carry out all of its responsibilities in these Supplier Licence Terms in a timely and efficient manner.

6.2 The Buyer acknowledges that the Supplier shall have no responsibility when Service Recipients and/or Authorised Users communicate with and/or undertake consultations with Patients using the Platform and:

6.2.1 agrees that it and each Buyer User shall retain clinical responsibility for these actions and for Patients in their use of the Platform; and

6.2.2 shall indemnify the Supplier against all costs, losses, damages, liabilities and claims, arising from or in relation to any third-party claims (including claims for clinical negligence) arising from the actions of Service Recipients and Authorised Users in providing services to Patients using the Platform, subject to the limitation of liability set out in the Order Form. In connection with any event reasonably likely to give rise to a liability under the indemnity in this clause 6.2.2, the Supplier shall give the Buyer written notice of any claim as soon as reasonably practicable.

6.3 The Buyer and the Supplier agree that the provisions of clause 6.2 do not fall within points 2(b) and 2(c) under the heading of *"Applicability of Supplier Terms"* in the Order Form as clause 6.2 establishes the agreed principle that a software provider cannot be responsible for an end user's actions.

6.4 The Buyer shall ensure that its network and systems and those of the other Service Recipients comply with the Minimum Requirements as necessary for the operation of

the Platform, Services and any Deliverables, and shall be solely responsible for procuring and maintaining all network connections and telecommunications links from its systems to the Supplier's data centres.

6.5 During the Contract Period and for a period of one year afterwards, the Buyer shall maintain in force insurance policies or indemnity schemes with reputable insurance companies or providers, against all risks that would normally be insured against by a prudent businessman in connection with the risks associated with this Contract and the provision of direct care services to Patients (including without limitation for medical negligence), and shall produce to the Supplier on request full particulars of that insurance and evidence that such insurance is current and in effect. The Buyer shall procure that the other Service Recipients comply with this clause 6.5 in respect of their risks.

6.6 The Buyer confirms it has understood, and procures that all Service Recipients and Authorised Users have understood, and agrees to the Product Disclaimers relevant to the Products to which the Service Recipients and Authorised Users have access. The Buyer agrees to bring the Product Disclaimers to the attention of any other Service Recipients and all Authorised Users.

6.7 If the Buyer has the right to carry out an Audit under this Contract (including, for the avoidance of doubt, in accordance with clause 6.3 of the General Terms), the Buyer:

6.7.1 may not conduct an Audit on the Supplier more than once in any Year; and

6.7.2 shall provide the Supplier with at least 30 days' written notice of any Audit and such notice shall confirm: a) whether any access is required to the Supplier's premises; b) what information is required as part of the Audit; c) the proposed date for the Audit so this can be agreed with the Supplier; and d) the identity of the Auditor.

7. Payment

7.1 The Buyer agrees to pay the Licence Fee and any Ancillary Fees:

7.1.1 in accordance with the Payment Terms and by the due date for the relevant invoice; and

7.1.2 from the Switch-on Date, unless otherwise stated in the Order Form or if the context otherwise requires.

7.2 The Licence Fee and any Ancillary Fees are stated exclusive of value added tax, which shall be added to the relevant invoice(s) at the appropriate rate where relevant.

7.3 In return for payment of the Licence Fee, each Service Recipient and their Authorised Users will be granted access to the Platform. These charges are non-refundable except

where another NHS organisation subsequently enters into a separate agreement with the Supplier for the Products and Service Recipients during overlapping periods. In such an instance, any refund will only be:

7.3.1 pro rata for overlapping contracted periods for the same Products and the same Service Recipients; and

7.3.2 made only to the relevant NHS organisation as agreed with the Supplier.

7.4 The Supplier may, without liability, and subject to Framework Special Term 7 and the required notice being provided to the Buyer, disable or suspend all Service Recipients' and Authorised Users' passwords, Accounts, access to all or part of the Platform until the invoice(s) concerned are paid in full. Interest shall accrue on a daily basis on any overdue amounts at an annual rate equal to 4% above the Bank of England's base rate, commencing on the due date and continuing until fully paid, whether before or after judgement.

7.5 The Supplier shall be entitled to increase the Licence Fee and, where relevant, any Ancillary Fees in accordance with any process set out in the Order Form.

7.6 The Buyer shall permit, and shall procure that the other Service Recipients shall permit, the Supplier to monitor the Platform in order to establish how many Authorised Users and Patients are using the Platform. If the Buyer has underpaid the Licence Fee, then without prejudice to the Supplier's other rights, the Supplier shall follow the process set out in clause 13.5.1 of the General Terms.

8. Compliance with Laws and Regulations

8.1 The Buyer shall, and shall procure that all Service Recipients and Authorised Users shall, comply with all applicable laws and regulations in the exercise of their rights and the performance of their obligations while accessing and using the Platform, Services and any Deliverables.

9. Intellectual Property Rights

9.1 As between the Buyer and Supplier, all Intellectual Property Rights in and to the Platform, Services, any Deliverables, the Accurx Documentation and the Analytical Data shall belong to, and remain vested in, the Supplier at all times.

9.2 Without prejudice to the generality of the foregoing and to the provisions of clauses 3.5 and 3.6 above, notwithstanding any rights or remedies of the Supplier, any and all Intellectual Property Rights in and to any Improvements to the Platform, Services and any Deliverables however arising shall immediately vest in and be owned by the Supplier without compensation or other obligation to the Service Recipients or any Authorised User. The Buyer shall procure the other Service Recipients' and Authorised Users' adherence to this clause 9.2. For the avoidance of doubt, any Improvements shall

not constitute New IPR or Specially Written Software (as defined by Joint Schedule 1 (Definitions)).

9.3 To give effect to clause 9.2, the Buyer shall, and shall procure that any other Service Recipients and all Authorised Users shall, assign to the Supplier all existing and future Intellectual Property Rights in the Improvements and all materials embodying these rights to the fullest extent permitted by law. Insofar as they do not vest automatically by operation of law or under this Contract, the Buyer holds legal title in these rights and Improvements on trust for the Supplier.

9.4 The Buyer undertakes to execute, and to procure that any other Service Recipients and all Authorised Users execute, all documents, make all applications, give all assistance and do all acts and things, at the expense of the Supplier and at any time either during or after the Contract, as may, in the opinion of the Supplier be necessary or desirable to vest the Improvements in the name of the Supplier.

9.5 The Supplier shall defend the Buyer against any third-party claims that the use of the Platform, Services and any Deliverables in accordance with these Supplier Licence Terms infringes any third-party Intellectual Property Right and, subject to clauses 9.6, and 9.7 shall indemnify the Buyer for and against any amounts awarded against the Buyer in judgment or settlement of such claims, provided that:

9.5.1 the Supplier is given prompt notice of such claim;

9.5.2 the Buyer provides reasonable co-operation to the Supplier in the defence and settlement of such claim, at the Supplier's expense;

9.5.3 the Supplier is given sole authority to defend or settle the claim; and

9.5.4 neither the Buyer nor any other Service Recipient makes any admission of liability or fault itself or on behalf of the Supplier.

9.6 In the defence or settlement of any claim pursuant to clause 9.5 above, the Supplier may at its sole option and expense either:

9.6.1 procure for the Buyer the right to continue using the Platform, Services and any Deliverables in the manner contemplated by this Agreement;

9.6.2 replace or modify the Platform, Services and any Deliverables as applicable so that it becomes non-infringing; or

9.6.3 terminate this Contract forthwith by notice without liability to the Buyer.

9.7 The Supplier shall not in any circumstances have any liability (including in respect of the indemnity provided under clause 9.5, any IPR claim and clause 10.5 of the General Terms) if the alleged infringement is based on:

9.7.1 modification of the Platform, Services and any Deliverables by anyone other than the Supplier or Improvements created independently by the Service Recipients or Authorised Users without input or written consent from the Supplier; or

9.7.2 the Service Recipients' and/or any Authorised Users' use of the Platform, Services and any Deliverables otherwise than in accordance with this Contract and/or the AUP or in a manner contrary to the instructions given to the Service Recipients by the Supplier; or

9.7.3 the Service Recipients' or Authorised Users' use of the Platform, Services and any Deliverables after notice of the alleged or actual infringement from the Supplier or any appropriate authority; or

9.7.4 use or combination of the Platform, Services and any Deliverables with any other software or hardware, in circumstances where, but for such combination, no infringement would have occurred; or

9.7.5 failure to meet the Minimum Specifications.

9.8 Subject to clause 9.7, the Buyer shall defend the Supplier against all or any costs, claims, damages or expenses incurred by the Supplier in respect of any third-party claims relating to the Service Recipients' or any Authorised Users' use of the Platform, Services and any Deliverables otherwise than in accordance with this Contract and/or the AUP, provided that the Buyer is given prompt notice of such claim.

10. Term and Termination

10.1 Without affecting any other right or remedy available to the Buyer or the Supplier, should the Buyer wish to add additional Service Recipients or Patients to this Contract, the Buyer and the Supplier will agree a variation to the Contract (in accordance with clause 27) which will take effect under the terms of this Contract and these Supplier Licence Terms.

10.2 Without prejudice to any other rights or remedies hereunder to which the Supplier may be entitled, if the Supplier knows or has reasonable grounds to suspect that any Buyer User or Authorised User is acting in breach of its obligations under these Supplier Licence Terms, the Supplier may suspend or disable the relevant Buyer User's or Authorised User's access to the Platform in accordance with Framework Special Term 7 if the Supplier considers that the conditions in Framework Special Term 7 have been met as a result of such breach.

10.3 On termination of this Contract for any reason:

10.3.1 all licences granted under this Contract shall immediately terminate and any

rights, remedies, obligations or liabilities of the Buyer and Supplier 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

10.3.2 the Supplier shall provide the exit assistance set out in the Exit Plan.

11. Limitation of Liability

11.1 Other than as expressly stated otherwise in this Contract, the Supplier makes no warranties, express or implied, including any implied warranties concerning merchantability or fitness for a particular purpose and all other 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 and without limitation, excluded from this Contract, and the Platform, Content, Services any Deliverables and the Accurx Documentation are provided to the Service Recipients on an 'as is' basis.

11.2 Nothing in these Supplier Terms excludes either the Buyer or Supplier's liability for death or personal injury caused by its negligence, fraud or fraudulent misrepresentation, or for any liabilities that cannot be excluded under applicable law.

11.3 Subject to clause 11.2:

11.3.1 the liability of the Buyer and Supplier whether in contract, tort (including negligence) or otherwise arising out of or relating to this Contract shall not exceed the limitation of liability set out in the Order Form; and

11.3.2 neither the Buyer or Supplier shall be liable for the losses excluded in clause 14.3 of the General Terms and the Supplier shall not be liable for any loss caused as a result of the Platform being unavailable caused by a Force Majeure Event.

12. Assignment

12.1 Neither the Buyer or the Supplier shall, without the prior written consent of the other, assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations in relation to the Platform, Services and any Deliverables under this Contract.

12.2 In the case of any Buyer Users merging with a third party, the Buyer shall give the Supplier at least thirty (30) days' written notice of any such merger and such notice shall:

12.2.1 include the name, address, national code (for example ODS code) of the proposed merger party that will assume engagement of the Buyer Users'

Authorised Users and the responsibility and care of its Patients; and

12.2.2 the date upon which such merger shall be effective.

12.3 The Buyer shall procure that the merger party in clause 12.2 agrees to meet all obligations of the relevant Buyer User under this Contract.

ANNEX A: PRODUCT DISCLAIMER (ACCURX MOBILE)

Accurx Mobile allows Authorised Users to access the Platform through a mobile application. One of the Products that Authorised Users can access within Accurx Mobile is a hospital directory of contacts which Authorised Users can access and update with mobile numbers and email addresses of contacts within a hospital (the **Directory**). Any information added to the Directory is information that is publically available to other Authorised Users accessing Accurx Mobile (**Public Content**), unless a Service Recipient requests that its Directory is kept private and requests to be the administrator of its Directory. Each Authorised User is responsible for the Public Content that they post, including the legality, reliability and appropriateness of the Public Content.

The Supplier does not supervise or moderate any Public Content whatsoever, and the Supplier has no liability or responsibility for Public Content. The Supplier reserves the right to remove or correct any Public Content. Service Recipients and Authorised Users acknowledge that Public Content will no longer be accessible if a Service Recipient has requested that the Supplier keep its Directory private.

By using Accurx Mobile, each Authorised User:

1. must respect the confidentiality of others, including colleagues and Patients;
2. must only publish publicly available data which is relevant for other healthcare professionals;
3. agrees that, by posting Public Content, they grant the Supplier and Service Recipient (where relevant) the right and licence to use, modify, publicly perform, publicly display, reproduce and distribute such Public Content on and through Accurx Mobile, and agree that this licence includes the right for the Supplier to make the Public Content available to other Authorised Users within Accurx Mobile, who may also use the Public Content subject to the Supplier AUP and this Product Disclaimer;
4. warrants that the posting of Public Content on or through Accurx Mobile does not violate the privacy rights, copyrights, contract rights or any other rights of any person, and agrees to contact the Supplier or the relevant Service Recipient if they are concerned about Published Content on any grounds whatsoever; and
5. agrees not to establish a link in such a way as to suggest any form of association, approval or endorsement by the Supplier where none exists.

Any Patient Data or Personal Data which is uploaded, submitted or collected via the Platform will be Processed by the Supplier (as Data Processor) in accordance with the Supplier DPA in line with the instructions provided by the relevant Service Recipient (as Data Controller).

ANNEX B: PRODUCT DISCLAIMER (ACCURX SCRIBE)

Accurx Scribe is provided by a third-party service (**Scribe Provider**) under and is subject to the other terms of this Contract and the following disclaimer applies to any access and use of Accurx Scribe.

1. Accurx Scribe is designed for use as a documentation aid only to assist with transcribing consultations and producing documentation. It is not to be used as a substitute for clinical diagnosis, treatment, or medical decision-making, all of which require skilled, professional human intervention and medical judgment or advice.

2. Neither the Supplier nor the Scribe Provider is responsible for any errors, omissions, or inaccuracies in the transcriptions produced by this third-party Artificial Intelligence (**"AI"**) service, or any unavailability of the Accurx Scribe feature. Neither the Supplier nor the Scribe Provider accepts liability for any misinformation or diagnosis based on or caused by any incorrect or inaccurate transcription arising from the use of Accurx Scribe and cannot guarantee the accuracy of transcriptions. All AI-generated content and outputs must be reviewed and verified before saving it to any clinical or medical/patient record systems.

3. Use of Accurx Scribe is therefore entirely at the Service Recipients' and Authorised Users' own option and risk. By using this feature, the Service Recipients and Authorised Users bear full responsibility for the final content added to any clinical or medical/patient record systems. Accurx Scribe does not provide medical advice and should never be used as a substitute for clinical knowledge, judgment, expertise or decision-making. The Service Recipients and Authorised Users should only make decisions that they would be comfortable making without the feature.

4. Accurx Scribe is designed primarily for use by the Service Recipients, Authorised Users and Patients with English as a first language. A translation feature is available within Accurx Scribe to assist Authorised Users undertaking consultations in a language other than English while documenting the consultation in English. This translation feature is not to be used as a replacement for an interpretation service or interpreter. This translation feature uses transcription and translation models available within the AI service (and current support languages are available at https://platform.openai.com/docs/guides/speech-to-text/supported-languages/#supported-languages, as may be updated from time to time). The accuracy of translation varies between available languages and the quality of the outputs generated by Accurx Scribe in languages other than English may be reduced. The Service Recipients and Authorised Users should ensure that all generated outputs and documents are checked for accuracy by an individual who both understands English and the language in which the consultation took place. Without this check, the accuracy of the output cannot be verified and the Supplier does not accept liability for any misinformation or diagnosis based on or caused by any incorrect or inaccurate

translation arising from the use of such translation features. Use of this translation feature is therefore entirely at the Service Recipients' and Authorised Users' own option and risk.

5. **Risks and Limitations.** AI and machine learning technologies, including Accurx Scribe, use emerging technology that may provide output that is inaccurate, is offensive, or is not designed or intended to meet the Service Recipients' and Authorised Users' needs, expectations, or legal, regulatory, or compliance obligations. The Service Recipients and Authorised Users acknowledge that with respect to their use of any Accurx Scribe feature, the Service Recipients are solely responsible for (i) developing their own internal policies on the appropriate use of these technologies and training Authorised Users or other relevant users on these policies, (ii) providing privacy notices and obtaining all necessary consents required by applicable laws, and (iii) implementing sufficient human oversight for the use of Accurx Scribe. Due to the nature of AI and machine learning technology, output may not be unique, and Accurx Scribe may generate the same or similar output for other customers. The Supplier does not guarantee the generation of output by Accurx Scribe. By using Accurx Scribe, the Service Recipients acknowledge and agree that neither the Supplier nor the Scribe Provider is responsible for (a) any inaccuracies or errors in the output from Accurx Scribe, (b) any biases, lack of fairness, or limitations of the underlying algorithms or data, or (c) any output that the Service Recipients or Authorised Users may find unsafe, harmful or offensive.

The Service Recipients and Authorised Users agree to contact the Supplier's user support team (support@accurx.com) if they encounter any issues with Accurx Scribe, so that these can be reviewed and resolved as quickly as possible.

Supplier Service Level Agreement

1. Definitions and Interpretation

1.1 Any capitalised words not defined within this Supplier Service Level Agreement shall take the meaning given to them under Joint Schedule 1 (Definition), unless specified otherwise.

1.2 For the avoidance of doubt, references to the “service levels” in this Supplier Service Level Agreement shall include “Key Performance Indicators" or "KPIs" (both as defined in Joint Schedule 1 (Definitions)).

2. Applicability

2.1 The following Supplier Service Level Agreement sets out the service levels on which the Supplier supplies the Platform (as defined in the Supplier Licence Terms) to the Buyer. The Buyer and the Supplier agree that this Supplier Service Level Agreement encompasses the service and performance levels and the related reporting required for the Platform under this Contract.

2.2 The following service levels shall:

2.2.1 not apply if the Supplier has provided the Buyer advance notice of any planned downtime and such planned downtime results in a loss of availability of the Platform;

2.2.2 only apply to the specific Products provided to the Service Recipients and their Authorised Users under this Contract.

2.3 The following shall be as set out in the Order Form: a) any Service Credits; b) the relevant Service Credit Cap; and c) a Critical KPI Failure.

3. Service levels for Accurx Scribe

3.1 The following service levels apply to Accurx Scribe (as defined in the Supplier Licence Terms):

Number	Metric	Definition	Target
1.	Note Accuracy	The portion of 250 randomly selected clinical notes generated by Tandem in the UK (the approved Subprocessor for Accurx Scribe as set out in the Supplier DPA), during each Month that do not contain Omissions or Hallucinations.	≥97%
2.	Transcription Latency	Median time taken between the end of recording and the completion of the transcript.	10 seconds
3.	Note Latency	Median time taken between the user	25

		clicking "Create Note" and the completion of the note.	seconds
4.	Uptime (Accurx) Scribe)	The system is considered up if new encounters can be started and, within 1 hour of finishing the consultation, it successfully generates the medical note and the note is available (i.e. retrievable and viewable in Accurx Scribe) to the Authorised User (as defined in the Supplier Licence Terms). If the note is not generated or not available within 1 hour, the system is considered down for that encounter.	99.9%

3.2 Definitions and information to be used in accordance with the service levels above:

Term		**Description**
Summarisation Errors		Errors introduced during the AI summarisation process. These are split into:
1.	*Hallucinations*	*1. Content added or misinterpreted by the summarisation that is not present in the original transcript (**Hallucination**).*
2.	*Omissions*	*2. Clinically relevant information present in the transcript that is missing in the summarised note.*

4. Service levels for Incident Response/Management

4.1 The Supplier shall aim to uphold the following service levels during an incident response, with adherence to these service levels reported to NHS England each Month.

4.2 Incident response times

4.2.1 The Supplier's engineers shall respond to urgent alerts within the following times:

When	**Response time**
Weekdays	10 minutes
Weekends	30 minutes

4.3 Incident resolution times

4.3.1 Incidents are assigned a Severity level according to the Supplier's incident management process and the Supplier shall aim to resolve incidents within the times set out below. Resolution times are calculated from declaration of the incident, to the time at which normal service levels are resumed.

4.3.2 Incidents that are assigned a Severity level of 1 or 2 are defined as High Severity Service Incidents (**HSSIs**) and are incidents where services are completely unavailable or severely degraded for Authorised Users. Severity levels 3, 4 and 5 are for incidents that affect the quality or performance of Accurx Scribe.

Severity	Resolution time
1	Within 2 hours
2	Within 4 hours
3	Within 72 hours (16 hours for clinical incidents with this Severity)
4	Within 144 hours
5	Within 336 hours

5. Services levels for User Support

5.1 "Core Hours" means:

5.1.1 Monday to Friday 8am to 8pm

5.1.2 Saturdays 9am to 5pm

5.1.3 Sundays and Bank Holidays 9am - 1pm

5.2 During Core Hours, the Supplier shall adhere to the following response times:

Contact Method	Response Time
Live Chat	Within 5 minutes*
Email	Within 2 hours*

**Where support tickets require escalation to Tandem's clinical support team, a response will be provided within 30 minutes.*

5.3 Phone

5.3.1 Users and patients can request a phone call via chat or email if that is their preferred method of communication during the above hours of operation.

5.4 Resolution

5.4.1 We aim to resolve issues raised by users to our user support team (through both webchat and email) within 12 hours during Core Hours.

5.5 Help Centre

5.5.1 The Supplier maintains a self-help centre (**Help Centre**) for its users which is

available and accessed via: https://support.accurx.com. The Help Centre provides hundreds of support articles, with walk-through guides, troubleshooting steps and FAQs, spanning our range of products and features to allow system users to self-help.

5.6 Complaints and Feedback Process

5.6.1 When an issue is escalated or a complaint is lodged via our complaints@accurx.com email, the Supplier will provide the user with a confirmation and with a case reference number within 48-hours of receiving the complaint.

5.6.2 If the complaint or query needs to be escalated, the case will be referred to the relevant team/s to be reviewed, who will then reach out to the user with further communications within 5 Working Days.

5.6.3 Should the investigation require further time and an extension of the 5 Working Days is required the Supplier will inform the user of this decision every 5 Working Days until the complaint response is submitted.

5.6.4 The Supplier aims to resolve issues as quickly as possible, however, depending on the complexity of the case, may require longer to investigate and resolve the issue. Nonetheless, the Supplier will aim to resolve all complaint cases within 30 Working Days.