



Note for signed copy:

The Accurx **Data Processing Agreement** is made available at <https://www.accurx.com/data-processing-agreement> and is incorporated into the Underlying Agreement, as defined and specified below.

For Healthcare Organisations that would like to receive a signed copy of the Data Processing Agreement with a list of approved sub-processors copied from Accurx's Sub-Processor Page, Accurx has made this copy available to them. The Healthcare Organisation does not need to sign and return this copy to Accurx. This copy includes signatures on the version of the Data Processing Agreement which was last modified on, and the list of approved sub-processors as of, 15 September 2026. No changes made to this copy are agreed to by Accurx.

Please note that Accurx may update the Data Processing Agreement from time to time and the current version of the Data Processing Agreement is available at <https://www.accurx.com/data-processing-agreement>. Previous versions of the Data Processing Agreement are available upon request from Accurx. Accurx's Sub-Processor Page may also be updated from time to time in accordance with the Data Processing Agreement and the current list of approved sub-processors is available at <https://support.accurx.com/en/articles/5501255-privacy-security-accurx-sub-processors>.

For any queries, please contact the Accurx team at support@accurx.com.

Accurx Data Processing Agreement

(DPA)

Last updated: 15 Sept 2026

This is an agreement ("Data Processing Agreement") between **Accurx Limited**, whose registered address at 7 Curtain Road, London, England, EC2A 3LT



(Company Registration Number: 10184077; ICO Registration Number: ZA202115; DSP Toolkit Organisation Code: 8JT17) (“**Accurx**”) and and the healthcare organisation using the Services (the “**Healthcare Organisation**”), each a “**Party**” and together the “**Parties**”.

Background

1. Accurx has developed a software application that consists of a range of products to support healthcare organisations. Accurx is used to communicate with and between patients, healthcare and/or social care professionals involved in the patient’s care.
2. The Healthcare Organisation is the Controller of, and appoints Accurx as its Processor to process Personal Data in order to provide the Services or an agreed subset of the Services (as defined below).
3. This Data Processing Agreement supplements and is incorporated into the underlying agreement between Accurx and the Healthcare Organisation (“**Underlying Agreement**”) and regulates the provision and use of Personal Data and ensures both Accurx and the Healthcare Organisation meet their obligations under the Data Protection Legislation.
4. In the event of any conflict or inconsistency between the provisions in this Data Processing Agreement and the Underlying Agreement(s), the provisions in this Data Processing Agreement shall prevail.



1. Definitions and interpretations

- 1.1. The following words and phrases used in this Data Processing Agreement shall have the following meanings, except where otherwise stated or the context otherwise requires:

Accurx's Sub-Processor Webpage	http://support accurx.com/en/articles/55012-55-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 Data Protection Act 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 Accurx 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 Healthcare Organisation Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems
Services	means the software services, or the agreed subset of the software services, provided by Accurx Ltd to the Healthcare Organisation; this software consists of a range of products to support communication with and between healthcare organisations and their patients;
Platform	means the range of products to support the communication with and between healthcare organisations and their patients developed, operated, and maintained by Accurx, and any ancillary products and services, that Accurx provides to Healthcare



	Organisations for its use in accordance with the terms of the Underlying Agreement
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

2. Scope of this Data Processing Agreement

- 2.1. This Data Processing Agreement applies to all data processing activities undertaken by Accurx as Data Processor on behalf of the Healthcare Organisation as Data Controller.
- 2.2. This Data Processing Agreement including the Schedules constitutes the written instructions of the Healthcare Organisation to Accurx to process Personal Data in the manner described herein. Such instructions may be supplemented by the Healthcare Organisation from time to time if, for example, the Healthcare Organisation elects to use a new Service offering provided by Accurx or decides to no longer use a particular element of the Services.

3. Duration and termination

- 3.1. This Data Processing Agreement shall remain in full force and effect for as long as the Healthcare Organisation continues to use the Services.
- 3.2. This Data Processing Agreement shall terminate automatically once the Healthcare Organisation and/or the healthcare and/or social care professionals that they employ no longer uses or has access to the Services. Notwithstanding the foregoing, the obligations in this Data Processing



Agreement 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 Data Processing Agreement or any associated agreements.

4. Obligations of the Data Controller

- 4.1. The Healthcare Organisation and Accurx acknowledge that, for the purpose of the Data Protection Legislation, the Healthcare Organisation retains control of the Personal Data and remains responsible for its 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 it gives to Accurx.
- 4.2. The Healthcare Organisation warrants and represents that its instructions to Accurx for the processing of Personal Data as contemplated under this Data Processing Agreement will comply with the Data Protection Legislation.
- 4.3. The Healthcare Organisation acknowledges that it is responsible for ensuring its use of Accurx to communicate with Data Subjects is appropriate and complies with Data Protection Legislation.
- 4.4. Schedule 1 has been reviewed and approved by the Healthcare Organisation 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 Data Processing Agreement; and



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

5. Obligations of Accurx

5.1. Processing Instructions

- 5.1.1. Accurx shall 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 Healthcare Organisation's instructions. Accurx will not process the Personal Data in any other way or in a way that does not comply with this Data Processing Agreement or the Data Protection Legislation. Accurx will notify the Healthcare Organisation immediately if, in Accurx's opinion, the Healthcare Organisation's instructions infringe Data Protection Legislation.
- 5.1.2. Accurx shall comply with any Healthcare Organisation instruction to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 5.1.3. Accurx shall maintain the confidentiality of the Personal Data and not disclose the Personal Data to third parties, unless the Healthcare Organisation or this Data Processing Agreement specifically authorises 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 Accurx to process or disclose the Personal Data to a third party, Accurx must first inform the Healthcare Organisation of such legal or regulatory requirement and give the Healthcare Organisation an opportunity to object or



challenge the requirement, unless the domestic law prohibits the giving of such notice.

- 5.1.4. Accurx shall delete or return all Personal Data to the Healthcare Organisation, at the choice of the Healthcare Organisation, as requested at the point of termination of this Data Processing Agreement and shall provide confirmation that all copies of the Personal Data have been deleted within ninety (90) days after termination of this Data Processing Agreement.

5.2. Rights of the Data Subject

- 5.2.1. Accurx shall, at no additional cost to the Healthcare Organisation, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Healthcare Organisation as the Healthcare Organisation may reasonably require, to enable the Healthcare Organisation to comply with:
- a) 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
 - b) information or assessment notices served on the Healthcare Organisation by the Information Commissioner's Office under the Data Protection Legislation.



- 5.2.2. Accurx must notify the Healthcare Organisation 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.
- 5.2.3. Accurx must notify the Healthcare Organisation within five (5) business 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 5.2.5, if Accurx receives a request or other correspondence from a Data Subject, and such communication relates to the Personal Data Accurx is processing on behalf of the Healthcare Organisation, Accurx 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 Healthcare Organisation. The provisions of this clause requiring Accurx to notify the Healthcare Organisation do not apply in circumstances where Accurx is unable to identify which Healthcare Organisation the relevant Data Subject is linked to (such as where the only information Accurx has about that Data Subject following a communication from them is an email address or mobile phone number).
- 5.2.4. Accurx will give the Healthcare Organisation its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.
- 5.2.5. Accurx must not disclose the Personal Data to any Data Subject or to a third party other than in accordance with the Healthcare



Organisation's written instructions, this Data Processing Agreement, or as required by domestic law.

5.3. Security Measures

5.3.1. Accurx shall 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 Schedule 2 ("**Security Measures**"). Accurx 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.

5.4. Compliance

5.4.1. Accurx will provide reasonable and timely assistance to the Healthcare Organisation to enable the Healthcare Organisation to comply with its obligations under the Data Protection Legislation, taking into account the nature of Accurx's processing and the information available to Accurx, 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.

5.4.2. Accurx shall appoint an individual within Accurx to act as a point of contact for any enquiries from the Healthcare Organisation relating



to the Personal Data Accurx is processing on behalf of the Healthcare Organisation. They can be contacted at dpo@accurx.com.

5.5. Audit

- 5.5.1. Accurx shall, upon the Healthcare Organisation's written request, make available such information as is reasonably necessary to demonstrate compliance with this Data Processing Agreement and Data Protection Legislation. Where such information is insufficient, the Healthcare Organisation may request an audit, subject to the following conditions:
- a) the audit shall relate solely to Accurx'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 Accurx's commercially sensitive information;
 - b) 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 Accurx's normal business hours, and in a manner that does not unreasonably interfere with Accurx's business operations;
 - c) the audit may be carried out by the Healthcare Organisation or a qualified independent auditor that is not a competitor of Accurx and is subject to Accurx's reasonable prior approval, such approval not to be unreasonably withheld or delayed;



- d) the auditor shall enter into a confidentiality agreement on Accurx's standard terms prior to commencing the audit;
- e) the Healthcare Organisation shall bear all costs and expenses of the audit, including Accurx's reasonable internal costs incurred in supporting the audit; and
- f) the results of the audit shall be treated as Confidential Information in accordance with the Underlying Agreement and used solely for the purpose of verifying compliance with this Data Processing Agreement.

5.6. Personal Data Breaches

- 5.6.1. Accurx must without undue delay (and in any event within forty-eight (48) hours) notify the Healthcare Organisation if it becomes aware of a Personal Data Breach.
- 5.6.2. Where Accurx becomes aware of a Personal Data Breach it shall, without undue delay, use its reasonable endeavours to provide the Healthcare Organisation with the following information:
 - a) 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;
 - b) the likely consequences; and
 - c) a description of the measures taken or proposed to be taken to address the incident, including measures to mitigate its possible adverse effects.



- 5.6.3. If Accurx cannot provide all the information above in the initial notification, Accurx will provide the information to the Healthcare Organisation as soon as it is available.
- 5.6.4. Accurx 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 Healthcare Organisation's written consent, except when required to do so by domestic law.
- 5.6.5. Accurx'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 5.6.5 do not apply to Personal Data Breaches that are caused by the Healthcare Organisation or its personnel that access the Services.

5.7. Accurx personnel

- 5.7.1. Accurx must ensure that Accurx personnel processing the data on Accurx's behalf are subject to a duty of confidentiality ensuring in each case that access is strictly limited to such personnel who need to access the relevant Personal Data, as strictly necessary to perform the Services in the context of that individual's duties to Accurx, ensuring that all such personnel:
 - a) are aware of and comply with Accurx's duties under this Data Processing Agreement;
 - b) 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 Healthcare Organisation or as otherwise permitted by this Data Processing Agreement;

- c) are subject to user authentication and log on processes when accessing the Personal Data; and
- d) have undertaken appropriate training in relation to Data Protection Legislation and in the use, care, protection and handling of the Personal Data.

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

6. Sub-Processors

- 6.1. The Healthcare Organisation gives Accurx a general written authorisation for the engagement of third-party sub-processors for the processing of Personal Data, subject to the terms of this Data Processing Agreement, Art. 32 of the UK GDPR, and the rules on transfers to third countries. The sub-processors currently in use by Accurx, and the locations in which processing occurs, are set out on Accurx's Sub-Processor Webpage and the Healthcare Organisation approves the engagement of such entities as sub-processors of Accurx for the processing of Personal Data. Accurx shall maintain an accurate list of its sub-processors currently in use on Accurx's Sub-Processor Webpage.
- 6.2. Accurx 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 Data Processing Agreement. Accurx will include terms in the



contract between Accurx and the sub-processor substantially similar to those set out in this Data Processing Agreement, and which are at a minimum compliant with the requirements of the Data Protection Legislation.

- 6.3. Accurx will not add or change any sub-processor processing Personal Data under this Data Processing Agreement without first informing the Healthcare Organisation of any intended change to Accurx's Sub-Processor Webpage concerning the addition or replacement of other sub-processors at least thirty (30) days in advance of when a new sub-processor for the processing of Personal Data is engaged.
- 6.4. The Healthcare Organisation 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 ten (10) business days following Accurx's notification to the Healthcare Organisation of the intended engagement with the new sub-processor. The parties agree to use good faith efforts to resolve the Healthcare Organisation's objection. Where an objection cannot be reconciled with the Service concept or technological requirements of Accurx, either party may terminate the applicable features of the Service with immediate effect. If no objection is received in accordance with this clause 6.4, the Healthcare Organisation will be deemed to have approved the engagement of the new sub-processor for the processing of Personal Data.
- 6.5. Where the sub-processor fails to fulfil its obligations under the written agreement with Accurx which contains terms substantially the same as those set out in this Data Processing Agreement, Accurx remains fully liable to the Healthcare Organisation for the sub-processor's performance of its agreement obligations.



7. Cross-border Transfers

7.1. The Healthcare Organisation consents to Accurx processing Personal Data outside the UK and/or the EEA provided that:

7.1.1. Accurx 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. Accurx shall identify on Accurx's Sub-Processor Webpage the territory that is subject to such adequacy regulations; or

7.1.2. Accurx participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that Accurx (and, where appropriate, the Healthcare Organisation) 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. Accurx shall identify on Accurx's Sub-Processor Webpage the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and Accurx must promptly inform the Healthcare Organisation of any change to that status; or

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

8. Liability

8.1. Accurx's liability arising out of or in relation to this Data Processing Agreement shall be subject to any limitation of liability provisions in the Underlying Agreement.

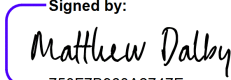


9. Governing law and jurisdiction

- 9.1. This Data Processing Agreement is governed by and construed in accordance with the laws of England and Wales.
- 9.2. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Data Processing Agreement, or its subject matter or formation.

10. Authority to enter into this Data Processing Agreement

- 10.1. If the party entering into this Data Processing Agreement with Accurx is an integrated care board or similar body acting on behalf of one or more Healthcare Organisations ("**Contracting Authority**"), the Contracting Authority represents that it is duly authorised to enter into this Data Processing Agreement on behalf of the Healthcare Organisations it represents and that such Healthcare Organisations will be bound by this Data Processing Agreement as if they were direct signatories to it.

Signed for and on behalf of ACCURX		Signed for and on behalf of HEALTHCARE ORGANISATION	
Signature:	Signed by:  750E7B960A2747E	Healthcare Organisation:	
Name:	Matthew Dalby	Signature:	
Title:	Data Protection Officer	Name:	
		Title:	
		Date:	



SCHEDULE 1: DATA PROCESSING DETAILS

1. Categories of Data Subjects

- Healthcare professionals, Authorised Users (as defined in the Underlying Agreement), and other individuals involved in accessing, providing, coordinating, supporting or improving health and social care services (“**Users**”).
- Patients and their carers, guardians, and representatives, as applicable (“**Patients**”).

2. Categories of Personal Data Processed

For Users:

- General contact information including name, email address, telephone number
- Workplace details including affiliated organisations, clinician ID, job role
- Metadata, event data, usage and behavioural data (such as edits to templates, and usage preferences and patterns)

For Patients:

- General contact information (including name, address, email, telephone number)
- Demographic details (including name, date of birth, gender)
- NHS number
- Special Category Personal Data, including data concerning Patients’ health processed via the Services (which may include consultation audio and/or video recordings, transcripts, patient images or documents, and other health data accessed via third-party services such as electronic medical records and other integrations such as PDS as applicable)

3. Subject matter

Accurx processes Personal Data on behalf of the Healthcare Organisation to provide the Services used by the Healthcare Organisation from time to time as described in the Underlying Agreement.

4. Duration of the processing



Accurx shall process the Personal Data for the duration of the Underlying Agreement on a continuous basis.

5. Nature and purpose of processing

Accurx may process Personal Data to provide the following categories of Services, where used by the Healthcare Organisation. For the avoidance of doubt, Accurx shall only process Personal Data as required to provide the specific functionality within the Services to which the Healthcare Organisation and its Users have access.

Service category	Processing activities
Core Services	Processing necessary to provide the Services and to maintain and improve the Platform including: • hosting, security monitoring, audit logging, system reporting, technical support, and deletion or disclosure of Personal Data in accordance with the Data Processing Agreement, Underlying Agreement, or applicable laws; • integrations with NHS and care systems, data matching, identity verification, and demographic checks against national and local healthcare registries such as PDS or Spine; • facilitating secure data exchange, record viewing and access, referrals, collaboration and care coordination, interoperability between authorised health and care systems, including without limitation across primary, secondary, community and social care settings; • processing necessary to carry out anonymisation, pseudonymisation, or aggregation of data (including the creation of Analytical Data as defined in the Underlying Agreement) and the subsequent use of such data for clinical safety, to improve platform performance and usability, and for product development. Note: Accurx may share anonymised statistics that it compiles about the use of the Services and Platform,



	such as the use of its functions by its users in communication with patients. Accurx may share these anonymised statistics with third parties, such as: • 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 such as relevant charities and academic institutions. Accurx may also compile and publish anonymised statistics and data about the use of the Services and Platform (for example as published findings and case studies on the responsible use and evaluation of AI within healthcare).
Care Navigation, Triage Services and Workflow Management	Receiving, structuring, classifying and routing patient requests, online consultation and triage submissions to support service-user prioritisation, clinical review, and signposting.
Patient Communication, Engagement and Telephony Services	Facilitation of inbound and outbound electronic communications, voice/telephony services, and video consultations between Users, Patients, and other service users, including automated notifications, appointment reminders, and booking, amending and cancelling appointments.
Consultation, Documentation and Coding Services	Capturing, receiving, transcribing, summarising, and coding clinical data. Generation of consultation notes, referral letters, and follow-up documentation to support direct care and clinical record-keeping.
AI-Supported Processing and Automation	Supporting the Services through automation, rules-based logic, machine learning, and artificial intelligence to assist in data classification, routing, drafting and validating processing outputs. 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 (including for the purposes of medical device regulation). Note: Outputs produced through AI-supported processing are intended to support the Healthcare Organisation and Users. The Healthcare Organisation and Users remain responsible for reviewing, approving, and relying upon such outputs in the delivery of care. Accurx shall not, and shall not permit any third-party sub-processor to, use the Personal Data to train or fine-tune general-purpose AI models unless expressly instructed by the Healthcare Organisation. Accurx may use the output generated by and the input provided to AI functionality in accordance with this Data Processing Agreement and the Underlying Agreement.
--	--

6. Sub-Processors

Accurx may use approved sub-processors to provide, support, secure, maintain and improve the Services.

Approved sub-processors are listed on Accurx’s [Sub-Processor Webpage](#), as updated in accordance with the Data Processing Agreement.

Accurx does not sell Personal Data and shall only share Personal Data with third parties (such as approved sub-processors) as set out in this Data Processing Agreement and for no other reason (for example, commercial gain).

7. Security measures

Accurx has implemented and will maintain appropriate technical and organisational measures to protect Personal Data as set out in Schedule 2.



SCHEDULE 2: TECHNICAL AND ORGANISATIONAL MEASURES

Security Measure	Detail
Measures of anonymisation, pseudonymisation and encryption of personal data	Personal data is protected through a combination of anonymisation, pseudonymisation, and encryption measures. Data no longer required for its original purpose is irreversibly anonymised; where linkage is needed for operational purposes, pseudonymisation is applied with identifier mappings held separately under strict controls. We do not attempt to re-identify individuals from any anonymised data or combine it with any other information about the same individuals. All personal data is encrypted at rest and in transit. Access to systems holding personal data is governed by role-based controls, limited to authorised and trained staff, protected by MFA, with privileged access granted on a temporary, approval-based basis only.
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 Business Continuity and Disaster Recovery (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 provider. 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	Accurx 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 Connect single sign-on for Accurx Web.
Measures for the protection of data during transmission	Data is transferred using a minimum of TLS1.2 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 change 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 Team; relevant systems are cloud-based, selected for high standards of technical and organisational security measures. Where possible, Single Sign-On (SSO) (with MFA) or MFA alone is enabled.
Measures for certification/assurance of processes and products	We hold ISO27001 certification and Cyber Essentials Plus. We are required to submit an annual NHS Data Security and 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. Accurx Scribe Outputs from Accurx Scribe are retained as identifiable Personal Data for a period of 90 days after creation. After 90 days outputs are permanently and securely deleted unless used for regression testing. Further details of these Processing activities and retention periods are set out in the relevant Data Protection Impact Assessment (DPIA) for



	Accurx Scribe, available in our Trust Centre .
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.



SCHEDULE 3: APPROVED SUB-PROCESSORS

Name	Nature and purpose	Location	Applicable features	International data transfer mechanism
Tandem Health AB (sub-processor to Tandem Health: ElevenLabs)	AI ambient voice technology Accurx Scribe enables healthcare professionals to focus on their patient rather than on note-taking during consultations. We engage Tandem Health AB to provide this feature; Tandem Health in turn uses ElevenLabs to perform the audio transcription of the clinician-patient consultation. Together, this pipeline listens to and transcribes the consultation, summarises it, and generates clinical content such as notes, referral letters, and patient letters. All data is processed and stored within the EEA. Recorded audio is deleted immediately after transcription is generated and is not retained by Tandem Health or ElevenLabs.	EEA	Accurx Scribe	Adequacy decision
Microsoft Azure (including Azure AI Foundry)	Cloud hosting service Accurx controls access to the infrastructure that we use to store and process the data on the platform. We use Microsoft Azure's secure cloud hosting service to securely store and process patient data. The Azure regions used are exclusively located in the UK, for both live and backup environments.	Azure: UK	Azure: All of Accurx	UK: N/A



	Azure AI Foundry Accurx uses Azure AI Foundry within the Azure environment to provide large language model capabilities to power certain AI features within the platform. Patient data processed by Azure AI Foundry is not used to train or fine-tune general AI models.	AI Foundry: EEA	AI Foundry: Smart Triage Questions (STQs)	EEA: Adequacy decision
FireText Communications Ltd.	SMS messaging provider Accurx enables users to send SMS messages to patients. We use third-party gateways for the delivery of those SMS messages. They provide APIs that the Accurx server uses to send these messages.	UK	Any Accurx messaging using SMS (including SMS Plus, Questionnaires, Batch, Appointment Reminders, Video)	N/A
BT Ltd	SMS messaging provider Accurx enables users to send SMS messages to patients. We use third-party gateways for the delivery of those SMS messages. They provide APIs that the Accurx server uses to send these messages.	UK and EEA	Any Accurx messaging using SMS (including SMS Plus, Questionnaires, Batch, Appointment Reminders, Video)	UK: N/A EEA: Adequacy decision
Vonage	SMS messaging provider Accurx enables users to send SMS messages to patients. We use third-party gateways for the delivery of those SMS messages. They provide APIs that the Accurx server uses to send these messages. Vonage is also a secure voice communications provider that Accurx uses to set up voice conversations between healthcare staff and their patients. No content of the call is recorded by Accurx, Vonage	UK and EEA	Any Accurx messaging using SMS (including SMS Plus, Questionnaires, Batch, Appointment Reminders, Video) Patient Call (select pilot practices only)	UK: N/A EEA: Adequacy decision



	or any other service. Technical logs are created to ensure Accurx and Vonage can monitor services and investigate any quality or technical issues. These are retained for a maximum of 90 days.			
NHS Mail	Secure email service Accurx uses secure NHS Mail accounts to send emails between healthcare professionals using the Accumail/Message GP feature.	UK	Accurx messaging using email (including Accurx – email patients, Accumail / Message GP)	N/A
Whereby Ltd.	Video consultation provider Whereby is a secure meeting room service that Accurx uses to host video consultations between healthcare and/or social care staff and their patients. No content of the call is recorded or retained by Accurx, Whereby or any other service. Technical logs are created to ensure Accurx and Whereby can monitor services. They are retained to allow Accurx and Whereby to investigate any issues with the service for up to 90 days.	EEA	Video	Adequacy decision
Sendgrid Inc.	Email campaign service provider Sendgrid is used within Accurx to send automated account emails to Accurx users only . This means Sendgrid only has access to email addresses of staff who use Accurx. No patient data is processed using Sendgrid.	EEA	All of Accurx	Adequacy decision



Intercom Inc.	Data Subject rights: user Support platform provider (not user support personnel who are provided by Accurx) Intercom provides a live chat, phone, and email communication platform that we use to interact with users whose patients exercise their data subject rights (e.g., data deletion requests). In these instances, it is the data controllers (our users) who provide us with the necessary information and instruct us on how to process it in order to fulfill the patient's request. Importantly, while patient data may be processed by Intercom in such cases, it does not include health data. Instead, it consists only of patient identifiers required to effectively process the request.	EEA	None, user support feature	Adequacy decision
---------------	--	-----	----------------------------	-----------------------------------