Data Processing Agreement

Contents

Overview

This is an agreement between the following parties:

- **The Data Controller:** Healthcare Organisation
- **The Data Processor:** AccuRx Ltd, 27 Downham Road, London, N1 5AA (Company Registration Number: 10184077; ICO Registration Number: ZA202115; DSP Toolkit Organisation Code: 8JT17)

Recitals

AccuRx is 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.

The Healthcare Organisation is the Data Controller in respect of certain Personal Data & Special Categories of Personal Data and appoints AccuRx Ltd as a Data Processor in relation to the provision of its Services agreed upon to process the data pertaining to Patients, health care or social care professionals involved in the Patient's care.

In order to provide the Services, AccuRx requires certain Personal Data & Special Categories of Personal Data to be made available by the Data Controller.

This Agreement regulates the provision and use of Personal Data, including Special categories of Personal Data, and ensures both AccuRx and the Healthcare Organisation meet their obligations under the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

1. Definitions and interpretations

1.1 The following words and phrases used in this Agreement, the Appendix or any Schedules shall have the following meanings except where the context otherwise requires:

AccuRx	the software service provided by AccuRx Ltd; this software consists of a range of products to support communication with and between healthcare organisations and their patients;
Anonymised data	means information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous (e.g. through aggregation) in such a manner that the data subject is not or no longer identifiable;
Data Controller	means a Person or Organisation who determines the purposes for which, and the manner in which, any Personal Data are, or are to be processed, in the case of this Agreement, the Healthcare Organisation;
Data Processor	in relation to Personal Data, means any Person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller which in the case of this Agreement is AccuRx;
Data Subject	means an individual to whom Personal Data, including Special Categories of Personal Data, pertains;
Data Recipient	means any person to whom the data are disclosed during the course of the data processing;
Electronic Patient Record System (EPR)	means the clinical system that holds the patient's electronic patient record, such as EMIS Web or TPP SystmOne;
The GDPR	means the General Data Protection Regulations (EU) 2016/679, a regulation in EU law on data protection and privacy for all individuals within the European Union;
GP Medical Record	means the patient's medical record held by their registered GP. GP medical records include information about a patient's medicine, allergies, vaccinations, previous illnesses and test results, hospital discharge summaries, appointment letters and referral letters;
Healthcare Organisation	is the healthcare and/or social care organisation providing direct care that uses AccuRx Services to process data pertaining to Patients in their care;
PDS	means the Personal Demographics Service, the national electronic database of NHS patient details such as name, address, date of birth and NHS number;
Person	recognised in law, that is to say individuals; organisations; and other corporated and unincorporated bodies of persons;
Personal Data	means any information relating to an identified or identifiable natural Person; an

	identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Special Categories of Personal Data	means revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;
Services	means the Services to be carried out by the Data Processor in order to provide AccuRx, and any other services that may from time to time be provided by the Data Processor, to the Data Controller.

2. The Agreement

2.1 This Agreement and its parts constitute written instructions of the Data Controller to the Data Processor to process personal data in the manner described in Schedule 1.

2.2 The Healthcare Organisation, the Data Controller, wishes to use AccuRx's services and AccuRx has agreed to provide these services according to instructions in this Agreement.

2.3 AccuRx, the Data Processor, is a software application that consists of a range of products to support healthcare or social care organisations. AccuRx is used to communicate with and between Patients, healthcare and/or social care professionals involved in the Patient's care.

3. Duration and termination

3.1 This Agreement shall remain in full force and effect while the Healthcare Organisation continues to use the Services.

4. Governing law

4.1 This Agreement is governed by and construed in accordance with the law of the United Kingdom

5. Obligations of the Data Controller

5.1 The Data Controller is responsible for the lawful basis for the processing of personal data, in particular with Schedule 1 of the Data Protection Act 2018.

5.2 The Data Controller must use AccuRx or another safe communications channel to communicate Personal Data and/or Special Categories of Personal Data to the Data Processor. The security of the channel used must correspond to the privacy risk involved.

5.3 The Data Controller must accept responsibility for use of content that it produces.

5.4 The Data Controller is responsible for the validity of any mobile numbers or emails entered by the Data Controller's staff.

5.5 The Data Controller must not rely on AccuRx for the communication of vital information. SMS messages should only be used to support and enhance communication. AccuRx provide no guarantees or assurances that SMS messages have been delivered or read by the recipient.

5.6 The instructions given by the Data Controller to the Data Processor in respect of the Personal Data/Special Categories of Personal Data disclosed to it by patients of the Data Controller or generated in respect of such patients shall at all times be in accordance with the laws of the United Kingdom.

5.8 The Data Controller must ensure that all data fields in AccuRx are correctly filled in and do not contain patient identifiable information where they are not supposed to.

5.9 The Data Controller, by entering into this Agreement, instructs the Data Processor to process the Personal Data/Special Categories of Personal Data on its behalf for the purpose of providing the Services, including the purpose of usage data reports in anonymised form.

5.10 The Data Controller, by entering into this Agreement, instructs the Data Processor to engage in reasonable monitoring of messages to prevent abuse, fraud or harm to patients through technical or user errors. This monitoring shall be proportionate and carried out through a person acting as a clinical lead.

6. Obligations of the Data Processor

Data Processing

6.1 Only process the Personal Data & Special Categories of Personal Data for the purpose of providing the Services and in accordance with the Data Controller's instructions.

6.2 Only process the Personal Data & Special Categories of Personal Data only to the extent and in such a manner as is necessary for the provision of the services.

6.3 Only process the Personal Data & Special Categories of Personal Data in compliance with the Data Protection Act 2018 and the GDPR.

Rights of the Data Subject

6.4 Assist the Data Controller in providing subject access and allowing data subjects to exercise all their other rights under the GDPR. The response to all subject information and other GDPR requests that may be received from the data subjects shall be provided within 14 days. All such requests must be received by the Data Controller and all communication with the Data Subjects must be via the Data Controller. If any requests are received by the Data Processor, the Data Subject would normally be instructed to contact the Data Controller.

Security Measures

6.5 Implement appropriate technical and organisational measures to protect the Personal Data, and any other Confidential Information, against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and/or other Confidential Information. As a minimum all data shall be encrypted in transit (with HTTPS via TLS 1.2 or higher) and at rest via Transparent Data Encryption (TDE);

Compliance

6.6 Assist the Data Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches, and data protection impact assessments.

6.7 Make available to the Data Controller all information necessary to demonstrate compliance with the obligations according to Article 28 of the GDPR and to allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

6.8 Delete or return all personal data to the Data Controller, at the choice of the Data Controller, as requested at the point of termination of the Agreement.

6.9 Notify all Customers of any information security breach or incident that may compromise the Personal Data & Special Categories of Personal Data covered by this agreement without undue delay after becoming aware of any such incident, taking into consideration the statutory breach reporting requirements and deadlines. The Data Processor shall work with the Data Controller to carry out a risk assessment and allow them to oversee and assess any corrective action.

6.10 To 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.

Confidentiality

6.11 To ensure that people processing the data are subject to a duty of confidentiality.

Sub-Processors

6.12 To only use the sub-processors listed in Schedule 2 of this Agreement. Schedule 2 may be modified unilaterally by the Data Processor as long as this complies with the requirements of Article 32 of the GDPR and the rules on transfers to third countries. Such changes to sub-processors shall be made available to the Data Controller. Where the change includes the change or an addition of a sub-processor, the Data Controller shall be given the opportunity to object. Where this objection cannot be reconciled with the Service concept or technological requirements of the Data Processor, the Data Processor may terminate the Agreement with immediate effect.

6.13 Not to store or directly transfer the Personal Data/Special Categories of Personal Data outside of the EEA without appropriate safeguards. However, we draw your attention to the fact that that:

- If either party to a communication (AccuRx users that send them, and their Patients) uses a device outside the EEA, then it may result in data being processed outside of the EEA.

Schedule 1
PROCESSING, PERSONAL DATA AND DATA SUBJECTS

Description	Details
Identity of the Data Controller and Data Processor	The Healthcare Organisation shall be the Data Controller and AccuRx Ltd shall be the Data Processor
Subject matter of the processing	To provide the Services. The AccuRx software requires certain Personal Data & Special Categories of Personal Data to be made available by the Data Controller.
Duration of the processing	The duration of the processing will be the duration of this agreement
Purposes and nature of the processing	The purposes of processing are health and social care purposes only. For the purpose of processing above, the nature of the processing may include, but is not limited to: ● Communication between patients, healthcare and/or social care professionals, via SMS, email, or other electronic communication, which may include images or documents. ● Sending links to surveys for patients to complete regarding their care. ● Video and audio communication for the purposes of video consultation, as outlined in Appendix 1. ● Healthcare and/or social care professionals using AccuRx may disclose patient data to the Data Processor when receiving technical support and from time to time the Data Processor'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. ● Compilation of anonymised statistics about the use of Data Processor's platform, such as the use of its functions by its users in communication with patients. These statistics may be used for the Data Processor's own analytics and improvement purposes. The Data Processor may also share these anonymised statistics publicly or with third parties. These third parties include: o national bodies, including NHS Digital and NHS England; o local NHS bodies, including CCGs and Primary Care Networks; o partners of the Data Processor, including commercial organisations, charities and academic institutions. ● In exceptional circumstances, the Data Processor may send a message to patients directly. For example in the event that the Data Controller has cancelled its agreement for AccuRx but patients remain using live Services, the Data Processor may text the patients to ask them to contact the Healthcare and/or Social Care Organisation for advice regarding next steps, prior to deleting or returning all the data according to Data Controller's instructions. ● Where applicable (in the case of a commercial agreement), the Data Processor may process personal data about the use of the platform and its features by the Data Controller's employees to determine billing amounts in line with such agreements.

Legal basis for processing	The Data Processor will process Personal Data for the purposes of the performance of the Agreement between the Data Controller and Data Processor. The Data Controller will ensure that they have the lawful basis to instruct the Data Processor to Process any Personal Data under this Agreement.
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 AccuRx (which may include patient images or documents and contain data concerning health). ● Other types of data (which may include contents of the patient's GP medical record and data concerning health that may from time to time be required to provide the Services).

Schedule 2
SUB-PROCESSORS

The Data Processor uses:

Name	Purpose	Entity Country	Contact Details
Firetext Communications Ltd.	A third-party SMS gateway for the delivery of SMS messages	England	• Website • Email
BT Ltd.	A third-party SMS gateway for the delivery of SMS message	England	• Website • Email
Microsoft Azure	Secure cloud hosting in accordance with NHS Digital guidance	England	• Website • Security Credentials Page
NHSmail	Process communications between healthcare and/or social care organisations	England	• Website • Email
TeamViewer UK Ltd.	To gain remote access and support over the internet [EU Compliant]	UK	• Website • Email
ActiveCampaign	As a CRM solution [EU Compliant]	US	• Website • Email
Intercom UK Ltd.	A messaging application for providing online user support [EU Compliant]	UK	• Website
Aircall	A web-based voice communication system for user support calls [EU Compliant]	US	• Website • Email
Whereby Ltd.	Host video consultations between healthcare and/or social care staff and their patients. See Appendix I for details.	UK	• Website • Security Credentials Page • Whereby's Data Processing Agreement
SendGrid	We use SendGrid for sending emails that don't contain patient identifiable information [EU Compliant]	US	• Website • Security Credentials Page

Appendix 1
VIDEO CONSULTATIONS

The video consultation service provided through the AccuRx platform is hosted by Whereby who are compliant with GDPR and based in the European Economic Area (EEA). A unique URL to the video consultation is generated and all participants are visible in the consultation, no third party can 'listen in'. The video and audio communication of the video consultation is only visible to participants on the call, and is not recorded or stored on any server (not AccuRx's, not Whereby's and not on any third party's servers).

All communication between participants' devices and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure websocket traffic or secure WebRTC). The video consultation connection either:

- connects participants to one another, relaying the encrypted data content through Whereby's TURN server, where it is not retained beyond this relay operation; or
- connects devices using 'peer-to-peer' connections between devices.

In both cases, as long as the participants are using their devices in the European Economic Area, it is guaranteed that any data is hosted and processed within the EEA, in line with NHS best practice guidelines on health and social care cloud security.

The data collected about patients is limited to that necessary to provide the meeting room service, and includes:

- Display name (if enabled and the user chooses to set one)
- Video meeting URL accessed
- Technical logs - information will be recorded in technical logs when the service is used. These logs will contain information such as, but not restricted to
    - IP address
    - Time of registered actions
    - Browser type and version

Technical logs are purged after 90 days, sufficient to allow AccuRx as the Data Processor to assist the Data Controller to complete investigations into data protection or clinical safety incidents.

Whereby's Data Processing Agreement (available on their Data Storage and Security page) details the commitments it makes to us when we contract with them as a sub-processor.