Data Processing Agreement

Between

- **The Data Controller:** Provider 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 health care or social care organisations. AccuRx is used to send messages to: Patients; health care or social care professionals involved in the Patient's care - both within and between Provider Organisations.

The Provider 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 Provider Organisation meet their obligations under the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

Definitions and interpretations

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

• *Provider Organisation* is the health care or social care organisation that uses AccuRx Services to process data pertaining to Patients in their care;

• *Data Controller* means a Person or Organisation who determines the purposes for which, and the manner in which, any Personal Data/Special Categories of Personal Data are, or are to be processed, in the case of this Agreement, the Provider Organisation;

• *Data Processor* in relation to Personal Data/Special Categories of 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;

• *AccuRx* the software service provided by AccuRx Ltd;

• *Person* recognised in law, that is to say individuals; organisations; and other corporated and unincorporated bodies of persons;

• *Data Subject* means an individual to whom Personal Data, including Special Categories of Personal Data, pertains;

• *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;
- *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.

The Agreement

This Agreement and its parts constitute written instructions of the Data Controller to the Data Processor to process personal data.

The Personal Data, including Special Categories of Personal Data, to be processed under this Agreement, includes but is not limited to the following data relating to **Patients of the Data Controller**, namely:

- Patient demographic details (name; date of birth; gender)
- NHS number
- Mobile phone number
- Email address
- Content of the communications with – or regarding - patients sent via AccuRx (which may include patient images or documents)
- Other types of data that may from time to time be required to provide the Services.

The Personal Data relating to **health care or social care professionals** involved in the Patient's care to be processed under this Agreement includes, but is not limited to:

- Name
- Email address
- Mobile phone number
- Content of the communications with – or regarding - patients sent via AccuRx (which may include patient images or documents)
- Other types of data that may from time to time be required to provide the Services.

Obligations of the Data Controller

- 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.
- The Data Controller must obtain all necessary consents in respect of patient data or ensure that another valid processing basis applies before entering such data. AccuRx will display the consent status of the Data Subject.
- The Data Controller takes responsibility for the validity of mobile number used, whether extracted from the medical record or manually entered.
- The Data Controller must not rely on AccuRx for the communication of vital information. SMS messages should be used to support and enhance communication. AccuRx provide no guarantees or assurances that SMS messages have been delivered or read by the recipient.
- 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.
- The Data Controller must accept responsibility for use of content that it produces.
- 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.
- 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 any metadata and usage data reports in anonymised form to AccuRx Ltd.

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

Obligations of the Data Processor

• To 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.

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

• To only process personal data in the scope of the written instructions of the data controller.

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

• To take appropriate measures to ensure all the aspects of technical and organisational security of processing according to Article 32 GDPR. All data shall be encrypted in transit (with HTTPS via TLS 1.2 or higher) and at rest (via TDE).

• To 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 20 working 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.

• To 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.

• To 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.

• To 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 controller.

• To maintain up-to-date compliance with the NHS DSP Toolkit. Our published report can be found under organisation code 8JT17.

• To retain data and information in the records for no longer than is necessary for the Data Processor to provide the Services, including using an audit trail, or to the extent necessary for the compliance with legal and with regulatory requirements.

• Users of 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.

• To only use the sub-processors listed in the Appendix. The Appendix 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.

• The Data Processor reports and collects metadata and usage data for the purposes of product and service improvement. To the extent it is in anonymised form, this data may be used for Data Processor's own analytics and improvement purposes.

• Not to store or directly transfer the Personal Data/Special Categories of Personal Data outside of the EEA without a lawful transfer mechanism. However, we draw your attention to the fact that that:
  - o A clinician who uses AccuRx to process patient data using a computer outside of the EEA may result in the data being processed outside of the EEA.
  - o A patient may be receiving messages whilst outside of the EEA.

• To 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 an 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.

• In exceptional circumstances, 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, Data Processor may text the patients to ask them to contact the Provider Organisation for advice regarding next steps, prior to deleting or returning all the data according to Data Controller's instructions.

Duration and termination

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

Governing law

This Agreement is governed by and construed in accordance with the law of England.

APPENDIX: SUB-PROCESSORS

The Data Processor uses:

- A third-party SMS gateway for the delivery of SMS messages. This service is provided by FireText or BT
- London Microsoft Azure secure cloud hosting in accordance with NHS Digital guidance
- NHSmail to process communications between provider organisations
- TeamViewer to gain remote access and support over the internet [EU compliant]
- ActiveCampaign as a CRM solution [EU compliant]
- Intercom a messaging application for providing online user support [EU compliant]
- Aircall a web-based voice communication system for user support calls [EU compliant]
- Whereby host video consultations between healthcare staff and their patients [EU compliant]

APPENDIX: VIDEO CONSULTATIONS

The video consultation service is hosted by Whereby who are fully 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 the user's browser, or the patient's browser, and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure websocket traffic or secure WebRTC). Furthermore, the video consultation connection prioritises 'peer-to-peer' connections between the clinician's and patient's phone over connections via their servers. In some cases, due to NAT/firewall restrictions, the encrypted data content will be relayed through Whereby's TURN server, but never recorded or stored. In such cases, as long as both the clinician and patient are using their computer devices in the European Economic Area, it is guaranteed that any data hosted on a server is within the EEA in line with NHS best practice guidelines on health and social care cloud security.

The only data related to the call that may be stored by Whereby is metadata to provide additional context about the way their service is being used. The usage data may include call participant's browser type and version, operating system, length of call, page views and website navigation paths, as well as information about the timing, frequency and pattern of the service use. The IP address of call participants may also be stored as part of this usage data. No other personal information of call participants is collected or stored by Whereby.