Spirit Product Use Review Service

Data Processing Agreement

2024

Spirit Implementers (or authorised contracted personnel) are subject to their relevant codes of practice and are accountable to the board of Spirit Implement Ltd (part of the Spirit Health Group Ltd)[1]. When pharmacists and nurses are engaged to deliver services, they are bound by the General Pharmaceutical Council (GPhC) or the Nursing and Midwifery Council (NMC) codes of conduct, respectively. All staff are accountable to the authorising GP in respect of clinical matters whilst working within the practice and will adhere to locally agreed protocols and guidelines.

Data Processing Agreement

This Data Processing Agreement is between Spirit Implement Ltd (the legally defined **Data Processor**), and the Practice as identified on Page 6 of this document **(Data Controller). (The Parties)**

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (GDPR)

This agreement is issued in accordance with the data protection principles of the Data Protection Act 2018 which is that everyone responsible for using personal data must make sure the information is:

- Used fairly, lawfully, and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant, and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than necessary
- Handled in a way that ensures appropriate security, including protection against lawful or unauthorised processing, access loss, destruction, or damage

Information to be processed by the Data Processor on behalf of the Data Controller

Data Subject

- Patients registered to the Data Controller, specifically those where a review service is agreed between the Data Controller and Data Processor
- Healthcare professionals involved in the patient's direct care

Data Class

The following information will be processed by the Data Processor:

- Patient name and address including full postcode
- Demographic data including but not restricted to
    - NHS number
    - Age

- Sex
- Health data - a range of clinical parameters relevant to the clinical conditions identified

1 Spirit Health and Spirit Implement are trading names of Spirit Health Group Ltd

Agreed processes between the Parties

The service will be delivered as outlined in the service introduction and clinical protocol, both of which have been supplied separately.

- Patient's personal and medication data is reviewed by Data Processor to provide continuing healthcare
- The patient is informed of any review outcomes and changes to care plan
- The Data Processor will update patients record on practice clinical system with outcomes of clinical reviews and changes authorised by the GP
- The Data Processor will provide summary reporting to the GP for authorisation detailing individual's actions and recommendations following:
    - Initial audit
    - Clinical reviews
    - On completion of the service
- The Data Processor will collate anonymised, amalgamated non-identifiable service data to support reporting to both Spirit Implement Ltd and where required, local NHS bodies e.g Integrated Care Board (ICB), Primary Care Networks (PCN).
- The Data Processor will report all adverse events identified by patients through the MHRA yellow card system www.mhra.gov.uk/yellowcard

Data Retention

The Data Processor will retain pseudonymised data (incl. EMIS number and initials) through delivery of the service and for a maximum period of three months following completion of the service for the purpose of maintaining an audit trail should any queries arise and require follow up. Following this, at the end of the three month period the data will be permanently deleted from Spirit SharePoint.

The Data Processor is not permitted to share the Data Controller's data with a third party other than non-identifiable data for reporting purposes as set out below. This will include, but is not limited to, the following:

- Sharing of the personal data with any other third party (unless for adverse event reporting as stated above)
- Publication of the personal data via any medium, including, but not limited to social media, websites, publicly available communications.
- Storing personal data on servers outside the UK.
- Granting third parties located outside the UK access rights to the Personal Data.

The Data Processor will retain & collate anonymised, amalgamated non-identifiable service data to support reporting to any company identified to the Data Controller as funding the cost of the service and where required, local NHS bodies e.g. Integrated Care Board or Primary Care Networks.

The Data Processor will only share the personal data with any third party with the express written permission of the Data Controller. Where express written permission has been granted, the data shall not be disclosed or transferred outside of the UK.

Data Security and Training

The Data Processor will be responsible for the security of transmission of any personal data in transmission and will ensure security by using appropriate technical methods.

The Data Processor agrees to implement appropriate technical and organisational measures to protect the personal data in their possession against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, including but not limited to:

- Ensuring IT equipment, including portable equipment, is kept in lockable areas when unattended.
- Not leaving portable equipment containing the personal data unattended.
- Ensuring that staff use appropriate secure passwords for logging into systems or databases containing the Personal Data.
- Ensuring that all IT equipment is protected by antivirus software, firewalls, passwords, and suitable encryption devices.
- Ensure that any sensitive personal data is stored and transferred (including where stored or transferred on portable devices or removable media) using industry (OWASP and NCSC guidelines) standard encryption or suitable equivalent.
- Limiting access to relevant databases and systems to those of its officers, staff agents and sub-contractors who need to have access to the personal data and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged by the Party.
- Conducting regular threat assessment or penetration testing on systems.
- Ensuring all staff handling personal data have been made aware of their responsibilities with regards to handling of personal data, with at least annual mandatory data protection training.
- Allowing for inspections and assessments to be undertaken in respect of the security measures taken or producing evidence of those measures if requested.
- Allowing for and contributing to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller in respect of the compliance of the Data Processor's processing of Data Controller personal data with the data protection laws.
- All data must be treated as confidential and held, shared and disposed of in line with all legal requirements and NHS guidance (including the Caldicott Guidelines).
- Data must be stored on a secure and encrypted server which will be backed up daily. Secure back up measures will be put in place to protect the confidentiality, integrity and availability of the back-up data.
- All data (including backups) must be stored within the UK.
- The service will be compliant with the NHS Data Protection and Security toolkit.

Any recommendations or advice will be kept in line with that laid out in the Department of Health Records Management Code of Practice

The Data Processor is under a strict obligation to notify any potential or actual losses of the transferred data to the Data Controller as soon as possible and, in any event, within two days of identification of any potential or actual loss to enable the data controller to consider what action is required to resolve the issue in accordance with the applicable national data protection laws and guidance.

Both parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any data security breach in a speedy and compliant manner.

Resolution of disputes with data subject of the Data Protection Authority

In the event of a dispute or claim brought by a Data Subject or the Information Commissioner's Office concerning the processing by the Data Processor's staff accessing the data, against either or both Parties,
the Parties will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion.

The Data Processor and the Data Controller agree to respond to any available non-binding mediation procedure initiated by a Data Subject or by the Information Commissioner's Office.

If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

In respect of data security issues relating to this agreement, each party shall abide by a decision of a competent court or of any binding decision of the Information Commissioner's Office.

Termination

Either party may terminate this agreement immediately by giving written notice of termination to the other party if the other party commits a material breach of this agreement.

Either party may terminate this agreement immediately by giving written notice of termination to the other party if the other party:

- Is dissolved
- Ceases to conduct all (or substantially all) of its business
- Is or becomes unable to pay its debts as they fall due
- Is or becomes insolvent or is declared insolvent; or convenes a meeting or makes or proposes to make any arrangement or composition with its creditors.
- An administrator, administrative receiver, liquidator, receiver, trustee, manager or similar is appointed over any of the assets of the other party.
- An order is made for the winding up of the other party, or the other party passes a resolution for its winding up (other than for the purpose of a solvent company reorganisation where the resulting entity will assume all the obligations of the other party under this agreement)

- Of if that other party is an individual.
  - The other party dies
  - As a result of illness or incapacity, that other party becomes incapable of managing his or her own affairs
  - That other party is the subject if a bankruptcy petition order

General

No breach of any provision of this agreement shall be waived except with the express written consent of the party not in breech.

If any provision of this agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of this agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part if it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect (unless that would contradict the clear

intention of the parties, in which case the entirety of the relevant provision will be deemed to be deleted).

The agreement may not be varied except by a written document signed by or on behalf of each of the Parties.

This agreement is made for the benefit of the Parties and is not intended to benefit any third party or be enforceable by any third party. The rights of the parties to terminate, rescind, or agree any amendment, waiver, variation, or settlement under or relating to this Agreement are not subject to the consent if any third party.

This agreement shall be governed by and construed in accordance with English Law.

The courts of England shall have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this agreement.