Data Processing Contract

BETWEEN

The Practice

(Hereinafter also known as the Data Controller)

AND

The Provider

Care Unbound ltd. trading as HERE, of 177 Preston Rd, Brighton BN1 6AG
(Hereinafter also known as the Data Processor)

In Support of

WorkFlow

Refer to email agreement or digital signature for date of THIS CONTRACT

WORKFLOW
by Practice Unbound

1 BACKGROUND INFORMATION

1.1 The Data Processor is Care Unbound ltd. trading as HERE hereafter known as HERE. The Data Processor has entered into a framework of co-operation and collaboration with Data Controller to provide services for Workflow.

1.2 Where the nature of those procured services requires the Data Processor to process Personal Data, the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation 2016 (GDPR) is engaged and establishes them as the Data Processor processing Personal Data on behalf of the Data Controller and legally responsible for that data processing under the Act.

1.3 Article 28.3 of the GDPR requires that processing by a Processor shall be governed by a contract or other legal act under Union or Member State law. The contract shall stipulate that the processor:

a) Processes the Personal Data only on documented instructions from the controller
b) Ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
c) Take all measures required pursuant to Article 32 of the GDPR
d) Respects the conditions referred to in paragraphs 2 and 4 or Article 28 or the GDPR for engaging another processor
e) Taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter 3 of the GDPR
f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the processor
g) at the choice of the controller, deletes or returns all the Personal Data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the Personal Data
h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

1.4 The Data Controller is receiving services from the Data Processor, which includes data processing to support the delivery of Workflow

1.5 This Contract is issued in accordance with Article 28.3 of the GDPR

1.6 There is a requirement upon the Data Processor to only process data as instructed by the Data Controller. The Data Controller remains legally responsible for the Personal Data even when it is processed by the Data Processor and therefore they must take steps to ensure the information assets remain protected, the liabilities and risks are appropriately managed, data is processed lawfully and the Contract is legally enforceable.

1.7 Service Level Agreements, Data Processing Agreements or an Information Sharing Agreement must not be used as an alternative to this Contract.

1.8 Certain words and expressions used in and are applicable to this Contract are defined in section 2 (below).

2 DEFINITIONS

Data Controller – As defined in Article 24 of the GDPR

Data Processor - As defined in Article 28 of the GDPR

Personal Data - As defined in Article 9 of the GDPR

3 DATA CONTROLLER RESPONSIBILITIES

3.1 The Data Controller is the Data Controller of the data insofar as it is Personal Data and, shall at all times, only process Personal Data lawfully and in accordance with DPA 2018 and GDPR principles.

3.2 It is the legal duty of the Data Controller to comply with the data protection principles in relation to all Personal Data with respect to which he is a Data Controller (unless an exemption applies). [1]

3.3 The Data Controller shall not instruct the Data Processor to process Personal Data on his behalf under this Contract where the Data Controller does not have a secure basis in law to process that data.

3.4 The Data Controller is legally responsible for the data processing carried out by the contracted Data Processor (HERE).

3.5 Article 28 (1) of the GDPR requires that the Controller shall use only Processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject

3.6 Article 28 (3) of the GDPR requires that processing shall be governed by a contract or other legal act

3.7 The Data Controller is entitled during the term of this Contract, to require the Data Processor to provide reasonable assurance that the technical and organisational security measures to protect the processing of Personal Data it is contracted to do. This includes the entitlement to audit the Data Processor's premises, systems, procedures, documents and staff as may be desirable or necessary to ensure compliance with this Contract and/or with the law.

4 DATA PROCESSOR RESPONSIBILITIES

4.1 The Data Processor is the Data Processor and shall at all time process Personal Data only as instructed to do so by the Data Controller and in accordance with the DPA 2018 and GDPR principles and the Contract.

[1] GDPR Art. 24

4.2 The Data Processor also undertakes to fully comply with all related and relevant legislation, regulatory and industry standards, including (but not limited to) the DPA 2018, GDPR, the Human Rights Act 1998 and the common law duty of confidence, the NHS Care Record Guarantee and the NHS Constitution.

4.3 The Data Processor shall have in place appropriate technical and organisational security measures equivalent to those imposed on the Data Controller by Art. 32 of GDPR

4.4 The Data Processor shall provide reasonable assurances and guarantees to the Data Controller as required that those technical and organisational security measures in place are both appropriate and effective in protecting the processing of Personal Data.

4.5 The Data Processor agrees to maintain good information governance standards and practices, by meeting or exceeding the requirements of the Information Governance Toolkit (or its successor), specifically to Level 2 in all requirements, and to share internal audit of the same on request.

4.6 The Data Processor shall not share the Personal Data with any third party without the prior written permission of the Data Controller or process Personal Data in any way or for any purpose that has not been instructed and authorised by the Data Controller.

4.7 Neither shall the Data Processor sub-contract a third party to process the Data Controller's Personal Data without the prior knowledge and written agreement of the Data Controller, and only then having provided all the necessary assurance and guarantees of their adequate organisational and technical security measures.

4.8 The Data Processor shall not transfer or permit the transfer of the Personal Data on to any territory outside the European Economic Area.

5 DATA SECURITY REQUIREMENTS

The Data Processor shall:

5.1 Have regard to the state of technological development and to the cost of implementing any measures, provide a level of security (including appropriate technical and organisational measures) appropriate to the harm that might result from unauthorised or unlawful processing of Personal Data or the accidental loss, damage or destruction of Personal Data and the nature of that Personal Data

5.2 Ensure that access to the Personal Data is limited to those employees who need access to meet the Data Processors obligations under this Contract

5.3 Take reasonable steps to ensure the reliability of the Data Processors' personnel who have access to the Personal Data, which shall include:

5.4 Ensuring that all staff engaged by the Data Processor understand the confidential nature of the Personal Data, and have received appropriate training in data protection prior to their use of the data, and have signed a written undertaking that they understand and will act in accordance with their responsibilities for confidentiality under the Contract.

The Data Processor shall ensure:-

5.5 That is has properly configured access rights for its staff, including a well-defined starters and leavers process to ensure appropriate access control

5.6 That suitable and effective authentication processes are established and used to protect Personal Data

5.7 That the Personal Data is backed up on a regular basis and that any back up data is subject to vigorous security measures as necessary to protect the availability, integrity and confidentiality of the data

5.8 That robust and tested business continuity measures are in place to protect the confidentiality, integrity and availability of the Data Controller's Personal Data.

5.9 Data is transferred securely where it is essential to do so in relation to this Contract and, ensure data transferred electronically is encrypted to the higher of the international data encryption standards for healthcare and National Standards (this includes data transferred over wireless or wired networks, held on laptops, CDs, memory sticks and tapes).

5.10 Employees are not able to access the data remotely e.g. from home or via their own electronic device or internet portal other than through a secure electronic network and in accordance with organisational remote working policy. No data shall be stored in such devices.

5.11 Where instructed by the Data Controller to dispose of data it is disposed of securely and confidentially in accordance with the secure destruction requirements specified in section 9

6 SERIOUS INFORMATION BREACH INCIDENT, INCIDENT REPORTING AND DUTY OF CANDOUR

6.1 The Data Processor shall have procedures in place to monitor access and to identify unauthorised and unlawful access and use of Personal Data.

62 The Data Processor shall immediately report any information security incident related to the Personal Data subject to this Contract to the Data Controller and undertakes to also fully cooperate with the Data Controller's incident investigation requirements.

6.3 In so far as the Data Controller is responsible for the Personal Data, it is the Data Controller's responsibility to ensure that the incident is reported in accordance with the Department of Health policy and procedures and for informing the relevant data subjects as appropriate.

7 PROCESS FOR AGREEING VARIATIONS

7.1 Any variation to the terms of this Contract shall be agreed in writing by the parties.

8 DISPUTE RESOLUTION PROCESS

8.1 Both parties shall aim to resolve all disputes, differences and questions by means of co-operation and consultation. Should this fail, then the dispute resolutions process in the standard NHS commissioning contract will be engaged – the conditions contained in GC8. Other terms of that contract will not be applicable in any way to this contract

9 SECURE DESTRUCTION

9.1 NHS data are subject to legal retention periods and should not be destroyed unless the Data Processor has received specific instruction to do so from the Data Controller. Where data has been identified for disposal:

9.1.2 The Data Processor shall ensure that NHS information held in paper form (regardless of whether originally provided by the Data Controller or printed from the Data Processor's IT systems) is destroyed using a cross cut shredder or subcontracted to a confidential waste company that complies with European Standard EN15713.

9.1.2 The Data Processor shall ensure that electronic storage media used to hold or process NHS Information is destroyed or overwritten to current CESG standards as defined at www.cesg.gov.uk

9.1.3 In the event of any bad or unusable sectors that cannot be overwritten, the Data Processor shall ensure complete and irretrievable destruction of the media itself.

9.1.4 The Data Processor shall provide the Data Controller with copies of all relevant overwriting verification reports and/or certificates of secure destruction of NHS information at the conclusion of the Contract.

10 EXIT FROM CONTRACT

10.1 The Data Controller may terminate this Contract with immediate effect by written notice to the Data Processor on or at any time after the occurrence of an event that gives rise to an information security incident or otherwise poses a risk of non-compliance with the data protection principles.

10.2 In order to protect the Personal Data, the Data Processor agrees:

10.2.1 To store and process Personal Data securely, and destroy it confidentially when it is no longer necessary and instructed by the Data Controller.

10.2.2 To return to the Data Controller any Personal Data held at the end of the Contract, ensuring secure transfer, or to makes arrangements for its secure disposal upon the instruction of the Data Controller.

11 LIABILITY AND INDEMNITY

11.1 Without affecting its liability for breach of any of its obligations under the service Contract, the Data Processor shall indemnify the Data Controller in full for costs, losses, charges, expenses it suffers arising out of the Data Processor's loss of the NHS Information or unauthorised or unlawful use of it whether arising in negligence or is otherwise a breach of this Data Processing Contract and including any fine imposed on the Data Controller by the Information Commissioner by way of civil monetary penalty (Art. 84 of the GDPR).

12 FREEDOM OF INFORMATION

12.1 The Data Processor acknowledges that the Data Controller is subject to the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).

12.2 In addition, the Data Controllers may be statutorily required to disclose further information about the contracted service or the Contract itself in response to a specific request under FOIA or EIR, in which case:

12.3 The Data Processor shall provide the Data Controllers with all reasonable assistance and co-operation to enable the Data Controllers to comply with its obligations under FOIA or EIR.

12.4 The Data Controllers shall consult the Data Processor regarding commercial or other confidentiality issues in relation to the Contract, however the final decision about disclosure of information or application of exemptions shall rest solely with the Data Processor.

DATA PROCESSING CONTRACT BETWEEN THE DATA CONTROLLER AND THE DATA PROCESSOR

On behalf of the Data Controller

Email response to this document will be taken as confirmation and approval

On behalf of the Data Processor

The Data Processor.....Here (Care Unbound)

Signed……

Name……Matthew Riley

Position……Information Governance Lead