South, Central and West Commissioning Support Unit

DATA PROCESSING AGREEMENT

Between

The Data Controller	
Practice name	
Practice code	

and

The Data Processor
NHS South Central and West CSU

Document information

Document type:	Operational Data Processing Agreement
Document title:	**Data Processing Agreement**
Document date:	November 2017
Author:	Information Governance Manager
Approved by:	NHS South, Central and West Commissioning Support Unit Information Governance Team
Approval date: Ratified by Corporate Business Committee:	
Version:	V1.1
Review date:	January 2021

Summary

This Data Processing Agreement is written between NHS South, Central and West Commissioning Support Unit (SCW) and Oxfordshire General Practices to demonstrate its role as Data Processor as identified in the relevant Information Sharing Agreements between Oxfordshire CCG and Oxfordshire General Practices, for whom the SCW provide analytic services.

Consultation

The Agreement has been overseen by the NHS South, Central and West Commissioning Support Information Governance Team.

THIS AGREEMENT

PARTIES	
Practice name	
Practice code	
AND	
NHS South, Central and West Commissioning Support Unit (SCW CSU)	
Headquarters	Omega House, 112 Southampton Road, Eastleigh SO50 5PB

Commencement Date: February 2018

Data Processing Agreement

1. INTRODUCTION

1.1 This agreement (the "Agreement") is intended to be an accountable operating framework to enable lawful disclosure of Data Controller information to the Data Processor in order to ensure that there are appropriate provisions and arrangements in place to properly safeguard the information entrusted to the Data Processor, including any Sensitive Personal Data.

1.2 SCW CSU is acting as Data Processor for the General Practices, working on their behalf to process data in accordance with their instructions.

1.3 Specific requirements for processing will be detailed in a schedule of Data Processing Schedules, which will formally establish relevant data management protocols and processes to ensure data is held and managed securely and in line with statutory requirements.

1.4 All references to NHS Digital refer to the directions made by the National Health Service Commissioning Board in relation to the establishment of information systems: Data Services for Commissioners under the relevant sections of the Health and Social Care Act 2012.

1.5 This agreement must be read in conjunction with the BOB overarching Data Sharing Agreement,

1.6 This agreement may be reviewed and amended to comply with the requirements of NHS England, NHS Digital, the Oxfordshire CCG and Oxfordshire General Practices and the statutory obligations of all organisations party to this agreement.

2. DEFINITIONS AND INTERPRETATION

2.1 In this Agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

(a) **"Anonymisation"** is the process of turning data into a form which does not identify individuals and where identification is not likely to take place.

(b) **"Confidential data"** shall mean any information or data in whatever form discussed, which by its very nature is confidential or which the Disclosing Party acting reasonably states in writing to the Receiving Party is to be regarded as confidential or which the Disclosing Party acting reasonably has marked as "confidential";

(c) **"Data"** shall mean all definitions of data processed on behalf of the Data Controller;

(d) **"Data controller"** has the meaning set out in section 1(1) of the DPA.

(e) **"Personal data"** shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic cultural or social identity;

(f) **"Personal confidential data"** shall mean any information relating to an identified or identifiable natural person ('data subject') and is owed a duty of confidence; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic cultural or social identity;

(g) **"Processing of 'Personal' and 'Personal confidential' data"** shall mean any operation or set of operations which is performed upon 'Personal' or 'Personal confidential' data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(h) **"Pseudonymisation"** is the process of de-identifying data so that a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without the individual being identified;

(i) **"Statute and Statutory Provisions"** is a reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time. A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

(j) **"Sub-contract" and "sub-contracting"** shall mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and "Sub Contractor" shall mean the party to whom the obligations are subcontracted; and

(k) "**Technical and organisational security measures"** shall mean measures to protect 'Personal' and 'Personal confidential' data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing.

3. OBLIGATIONS OF THE DATA PROCESSOR

3.1 The Data Processor shall only carry out those activities in respect of the data processed on behalf of the Data Controller as expressly authorised by the Data Controller.

3.2 The Data Processor shall take such technical and organisational security measures as are required under law to protect data against unlawful forms of processing.

3.3 The Data Processor will ensure as a minimum, compliance with the legal and practical security requirements set out in the relevant version of the NHS Information Governance toolkit..

3.4 The Data Processor will not further process or use data obtained in its role as processor other than as instructed by the Data Controller.

3.5 The Data Processor shall comply with the security, confidentiality and other obligations imposed on it under this agreement and in accordance with any requirements detailed in relevant agreements covering processing of the data.

3.6 The Data Processor will not access, process or use data provided outside of the European Economic without the prior written permission of the Data Controller.

3.7 The Data Processor will maintain a Privacy Notice detailing the processing undertaken as part of this agreement.

3.8 All data will be stored securely regardless of the media that it is held on. Physical security controls will be in place to prevent unauthorised access to paper based information and electronic access controls will be in place, where all users with access to data will have their own unique username and password (or where required Smartcard).

3.9 Data will only be put on mobile devices and removable media if absolutely necessary and will be encrypted to industry standards at all times. In preference for placing data on removable media, secure file transfer tools will be used for any necessary transmission of data.

3.10 SCW CSU will only hold data for the minimum period of time and in accordance with the period stipulated within any relevant sharing agreement. When information is no longer needed it will be deleted in accordance with SCW CSU records management procedures.

3.11 SCW CSU will ensure that all members of staff receive ongoing training in the handling of 'Personal' and 'Personal confidential' data. This will be in accordance with the standard NHS requirements under the NHS Information Governance toolkit.

3.12 Data processed will be subject to the appropriate techniques to render it non-identifiable. These include anonymisation and pseudonymisation. Data will also be processed at patient level only where it is rendered non-identifiable, unless it is for direct patient care.

4. OBLIGATIONS OF THE DATA CONTROLLER

4.1 Processing of 'Personal' and 'Personal confidential' data will only be requested where there is a legal basis for the use of such data. All processing will be in accordance with the relevant Data Sharing Protocol and the General Practices' obligations under the Data Protection Act 1998 and other relevant legislation including the GDPR legislation due to come in force in 2018.

4.2 The Data Controller will provide comprehensive information to Data Subjects by way of a Privacy Notice which clearly identifies the data sharing relationships and identifies SCW as the Data Processor.

4.3 Use for any activity outside the current remit of the relevant Data Sharing Protocol, the Data Controller will obtain specific approval and consent from other parties prior to requesting SCW to process it. The General Practice's Caldicott Guardian, or SIRO where applicable, will be responsible for ensuring that approvals are sought and relevant sharing agreements are signed on behalf of the General Practice.

5. DATA SUBJECT ACCESS RIGHTS

5.1 The Data Processor acknowledges that individuals have a right to see what personal data is held about them, and to know why and how it is processed.

5.2 The Data Controller has an obligation to respond to these requests.

5.3 The Data Processor agrees to notify the Data Controller in the event that it receives a subject access request or notice from a data subject exercising his rights under the DPA in relation to the Data Controller data or any correspondence from the Information Commissioner in relation to the processing of the Data Controller data.

6. CONFIDENTIALITY

6.1 The Data Processor agrees that it shall maintain 'Personal' and 'Personal confidential' data in confidence (where that duty is owed). In particular, the Data Processor agrees that it shall not disclose any data covered by this agreement to any third party unless:

(a) It is instructed to do so by the Data Controller; or

(b) Information is in the public domain or is required to be disclosed by law such as in safeguarding situations.

6.2 Nothing in this agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

6.3 All parties to this agreement will have due regard to the following guidance on the processing of 'Personal' and 'Personal confidential' data:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

http://systems.NHS Digital.gov.uk/infogov/codes/cop/code.pdf

https://ico.org.uk/for-organisations/guide-to-data-protection/

https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

7. SUB-CONTRACTING

7.1 The Data Processor shall not sub-contract any of its rights or obligations under this Agreement without the prior written consent of the Data Controller.

7.2 Where the Data Processor is permitted to sub-contract its obligations under this agreement it shall do so only by way of a written agreement with the Sub-Contractor which imposes the same obligations in relation to the security of the processing on the Sub-Contractor as are imposed on the Data Processor under this agreement.

7.3 Where the Sub-Contractor fails to fulfil its obligations under any sub processing agreement, the Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this Agreement.

8. DATA TRANSFER PROCESSES

8.1 Relevant data will be provided to SCW according to the Data Transfer Method identified in the relevant Data Sharing Protocol.

9. INCIDENT MANAGEMENT

9.1 The Data Processor shall notify the Data Controller immediately (in any event within 24 hours) of any untoward incidents or activities that suggest non-compliance with any of the terms of this Agreement. This includes 'near miss' events even if no actual damage to or loss -or inappropriate disclosure of Data results.

9.2 It is the responsibility of the Data Controller to report the incident to NHS Digital where appropriate. Any incident will be assessed in terms of severity using the NHS Digital Information Governance Serious Incident Requiring Investigation framework as identified in the NHS Digital Information Governance Toolkit.

10. COMMENCEMENT, DURATION AND REVIEW

10.1 This agreement will commence on 3 January 2018 and will take effect for a period of 3 years, unless reviewed earlier.

10.2 The Data Controller may terminate this Agreement by giving to the Data Processor not less than one months' written notice expiring at the end of the relevant period of three months.

10.3 The Data Controller may terminate this Agreement with immediate effect by written notice to the Data Processor on or at any time after the occurrence of an event specified below:

(a) The Data Processor is in material breach of this Agreement and that breach cannot be remedied; or

(b) The Data Processor is in material breach of this Agreement which can be remedied but the Data Processor fails to do so within 30 days starting on the day after receipt of the written notice from the Data Controller referred to in clause 10.2;

(c) It becomes unlawful for the Data Processor to perform all or any of its obligations under this Agreement.

11. AUDIT

11.1 The Data Processor shall keep detailed, accurate and up-to-date records relating to the processing of the Data on behalf of the Data Controller as part of organisational and business level mapping of Data Flows.

11.2 The Data Processor will make available records relating to this agreement to the General Practices under the relevant Data Sharing Protocol where required.

.

12. INTELLECTUAL PROPERTY RIGHTS

12.1 The Data Processor acknowledges that it shall have no rights in or to the data provided under the relevant Data Sharing Protocol other than the right to use it for the provision of services identified within the relevant Data Sharing Protocol.

12.2 All parties recognise that NHS Digital retains copyright of any NHS Data provided under any relevant sharing agreement.

13. JURISDICTION

13.1 Each party irrevocably agrees that the courts of the United Kingdom shall have exclusive jurisdiction to settle any dispute or claim arising out of, or in connection with, this agreement or its subject matter or formation (including non-contractual disputes or claims and the governing law for this agreement shall be that of the United Kingdom).

14. CHANGE MANAGEMENT AND GOVERNANCE

14.1 Any minor changes to this Agreement that may be deemed necessary from time to time by the Data Controller, or requested by the Data Processor and approved by the Data Controller, shall only be valid once issued in writing and signed by both parties.

14.2 In proposing or assessing any relocation, upgrade or change, the Data Processor will evaluate the impact on data privacy and security and advise the Data Controller of any new or increased threats or

vulnerabilities that could result from such relocation, upgrade or change and the Data Processor will propose policies to protect the Data Controller from such threats or vulnerabilities.

SIGNATORIES

DATA CONTROLLER

Signed by ……..

Name:

Position: Caldicott Guardian/Senior Information Risk Owner or delegate

Date:

On behalf of: (insert General Practice name)

DATA PROCESSOR

Signed by ……..

Name:

Position:

Caldicott Guardian/Senior Information Risk Owner or delegate

Date:

On behalf of: NHS South, Central and West Commissioning Support Unit