Data Processing Agreement

BETWEEN

Chirk Surgery
(Acting as Data Controller)

AND
Shropshire Clinical Commissioning Group
Referral Assessment Service (RAS)
(Hereinafter known as the Data Processor)

Table of Contents

1.0 Introduction

1.1 This Agreement provides an operating framework to enable lawful disclosure of NHS information to and data processing by the Data Processor working on behalf of the Data Controller taking account of the Data Protection Act 1998, and NHS guidance on confidentiality of personal information, the common law duty of confidence and other applicable legislation. This document takes account of the Health and Social Care Act 2012 and the requirement of processing PCD (Personal Confidential Data) in accordance with the Act, s.256 of the NHS Act 2006.

1.2 The terms and conditions of this Agreement shall apply to all NHS information provided by the Data Controller, or obtained by the Data Processor from other sources as part of the delivery of the contracted services, or derived from any combination thereof.

1.3 This Agreement between the Data Controller and the Data Processor supports and is specific to *the services mentioned in 4.2*

1.4 This agreement covers all activity signed off in section 4.2 – this gives the data controller the choice to indicate which services they would like to contribute to.

2.0 Definitions

2.1 **Personal data*** any factual information or expressions of opinion relating to an individual who can be identified directly from that information or in conjunction with any other information that is held by or comes into the possession of the data holder.

2.2 **Sensitive personal data*** the eight categories of personal information defined as sensitive personal data in section 2 of the Data Protection Act 1998 (DPA) and, in this Agreement specifically including (but not limited to) information about the physical & mental health, racial or ethnic origin, sexual life or sexuality of patients or service users.

2.3 **Confidential Information*** any information or combination of information that contains details about an organisation or an individual person that was provided in an expectation of confidence. This includes for example, non-personal corporate or technical information that is commercially sensitive, drafts of documents that are not ready for publication, restricted information & documents, etc. as well as personal data about patients, service users and staff.

2.4 **NHS information*** any information as defined in 2.1 to 2.3 above that the Data Controller owns. This includes all information supplied to the Data Processor by the Data Controller and any additional information that the Data Processor obtains during the term of the contract and shall apply equally to original NHS information and all back-up and/or copies printed out.

2.5 **Data Controller*** as defined in the Data Protection Act (1998) is the individual or organisation (legal person) who determines the manner and purpose of the processing personal information, including what information will be processed and how it will be obtained.

2.6 **Data Processor*** as defined in the Data Protection Act 1998, is an individual (other than an employee of the data controller) or organisation who processes personal information whilst undertaking a business activity or service on behalf of the Data Controller, under contract.

2.7 **Data Processing*** also defined in the Data Protection Act 1998 in respect of personal data, for the purpose of this document this includes any business activity or

contracted service that involves using personal, corporate or other information including obtaining, recording, holding, viewing, storing, adapting, altering, deleting, disclosing. This is not restricted to computer processing, but includes manual files and verbal discussions.

2.8 **Personal Confidential data** This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this report 'personal' includes the Data Protection Act 1998 s.1 definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive personal data' as defined in the Data Protection Act 1998. This term was introduced in the Caldicott 2 review and is not the term used across the Health economy.

3.0 General

3.1 The Data Processor shall put in place appropriate technical and organisational measures to ensure the protection of the information subject to this Agreement against the accidental loss or destruction of or damage to NHS information, having regard to the specific requirements set out in this Agreement, the state of technical development and the level of harm that may be suffered the Data Controller and/or by a Data Subject whose Personal data is affected, by such unauthorised or unlawful processing or by its loss, damage or destruction.

3.2 All NHS information referred to in 2.4 above remains the property of the Data Controller and shall be either returned or destroyed by the Data Processor after a period of [insert agreed retention period] after completion of the contracted service, in a manner previously agreed with the Data Controller.

3.3 Under the terms of this Agreement the Data Controller shall provide the Data Processor with the minimum amount of NHS information necessary to deliver the contracted service and, in particular, personal and sensitive information will be supplied on a restricted 'need to know' basis.

3.4 The Data Processor shall only process NHS information as is necessary to perform its obligations under this Agreement and only in accordance with any instruction given by the Data Controller under this Agreement and, in particular shall not use or process NHS information for any purpose other than as directed by the Data Controller for delivery of the contracted service.

3.5 The Data Processor shall not subcontract any of its processing operations performed on behalf of the data controller under this Agreement without the prior written consent of the Data Controller. Where the Data Processor subcontracts its obligations, with the consent of the Data Controller, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data processor under this Agreement. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data processor shall remain fully liable to the data controller for the performance of the sub-processor's obligations under such agreement.

3.6 Any minor changes to this Agreement that may become necessary from time to time shall be made by the Data Controller to the Data Processor, or requested by the Data Processor from the Data Controller, as a written variation.

3.7 In the event of major changes being required, the Data Controller shall terminate this Agreement and replace in full with an updated version. Such termination and

replacement may also be initiated by the Data Processor, subject to prior arrangement with the Data Controller.

4.0 Description of NHS information

4.1 The NHS information covered in this Agreement is as detailed in section 4.2 and where relevant is indicated as personal, sensitive or confidential as defined in sections 2.1, 2.2 and 2.3 respectively. The Data Processor shall not disclose information to any third party without the prior written agreement of the Data Controller. Disclosure of such data as may contain patient information will require evidence of Caldicott Guardian approval before disclosure for the purpose of delivery of the contracted service. Any data will require evidence of authorised manager\or Caldicott Guardian approval (as appropriate) before disclosure for the purpose of delivery of the contracted service.

4.2 The NHS information covered in this Agreement is as detailed below:

This data Processing agreement is set up between

- Shropshire CCG (RAS)
- Chirk Surgery

The Practice will share with RAS the data in patient records as below. The records will be shared with and utilised for the purpose of patient contact to facilitate the referral of the patient to a secondary Care organisation which will lead to the consultation with and treatment of the individual patients. The defined purpose for RAS to have Patient records shared with them by the practice is to provide “Non- Direct Patient Care” as defined in the Caldicott 2 Review 2012, the patient confidential Data (PCD) (information that identifies the patient) will only be used by RAS staff who have a legitimate powers to access the data, by having the explicit consent of the patient. The consent of the patient must be recorded at the time of RAS consultation.

RAS will share with the Practice the data as below for the purpose of review by a Practice GP and update of patient records maintained by the Practice at the Practice GPs discretion; and to inform future consultations with and treatment of the individual patients.

The services sharing this data within RAS may from time to time change and any changes will be reflected in a Change notice. Secondary agreement from Practices will not be sought when new services use the data as the use will still be within the definition of the processing above, practices at any time can actively dissent to sharing their data with RAS, but this should be rarely applied as this would impact upon patient service and safety.

The parties to this agreement may only use the information disclosed to them under this agreement for the specific purpose(s) set out in this document. The information will not be shared with, or passed to, any third parties without prior approval of the originating partner’s Data Controller.

Information to be shared

Information to be shared by the Practice:

Type of Sharing Agreement	Function
Demographic/ PCD	Only core patient demographic information including Name, Address, DOB, Gender, NHS number, Usual GP, Ethnicity and Marital Status
Care Record	Summary, Consultations, Medication, Problems, Investigations, History, Diary and Appointments, Attachments, Referrals, Warnings and Care Plans

Exclusions

Additional Secondary uses of PCD are not allowed by this sharing agreement, in accordance with the Health and Social Care Act 2012 only the clinical team providing direct patient care with the consent of the patient will have access to identifiable patient data. Free text fields on the GP system will also be excluded from the data accessible by RAS.

Information to be shared by RAS

Type of Sharing Agreement	Function
Demographic/ PCD	Only core patient demographic information including Name, Address, DOB, Gender, NHS number, Usual GP, Ethnicity and Marital Status
Care Record	Summary, Consultations, Medication, Problems, Investigations, History, Diary and Appointments, Attachments, Referrals, Warnings and Care Plans

Exclusions

Additional Secondary uses of PCD are not allowed by this sharing agreement, in accordance with the Health and Social Care Act 2012 only the clinical team providing direct patient care with the consent of the patient will have access to identifiable patient data.

4.3 All data will be sent from the GP practice to the RAS via the Welsh Clinical Commissioning Gateway (WCCG).

5.0 Data Protection

5.1 The Data Processor shall comply with all aspects of the DPA, Human Rights Act 1998 and common law duty of confidentiality in relation to the processing of personal data and sensitive personal data as part of this Agreement

5.2 The Data Processor shall only process data in accordance with the instruction of the Data Controller as specified under this Agreement

5.3 The Data Processor shall put in place appropriate technical and organisational measures against any unlawful and unauthorised processing of NHS information and against accidental loss, destruction of and damage to NHS information.

5.4 The Data Processor shall not cause or allow NHS information to be transferred to any territory outside the European Economic Area without the prior written permission of the Data Controller.

5.5 All recorded information held by public sector agencies is subject to the provisions of the Freedom of Information Act 2000 and the Data Protection Act 1998. While there is no requirement to consult with third parties under FOIA, the parties to this agreement will consult the party from whom the data originated and will consider their views to inform the decision making process. All decisions to disclose must be recorded by the disclosing organisation.

Each Partner Organisation shall publish this agreement on its website and refer to it within its Publication Scheme. If a Partner Organisation wishes to withhold all or part of the agreement from publication it shall inform the other Partner Organisations as soon as reasonably possible. Partner Organisations shall then endeavour to reach a collective decision as to whether information is to be withheld from publication or not. Information shall only be withheld where, should an application for that information

be made under FOIA 2000 it is likely that the information would be exempt from disclosure and the public interest lie in favour of withholding. However, nothing in this paragraph shall prevent the individual Partner Organisations from exercising its obligations and responsibilities under FOIA 2000 as it sees fit.

5.6 Subject access requests will be dealt with on a case by case basis by the organisation which receives the request in line with their policies and procedures

5.7 Each organisation will inform members of the public via their Fair Processing Notice which is made publically available upon request.

6.0 Policies and Procedures

6.1 The Data Processor shall have confidentiality, information security, data protection and records management policies. These will describe individual responsibilities for handling NHS information and will be rigorously applied.

6.2 The Data Processor shall provide the Data Controller with copies of the policies referred to in 6.1 above on request *or* as appendices to this Agreement.

7.0 Data Processor Employees

7.1 The Data Processor shall undertake all reasonable background checks to ensure the reliability of all employees who are likely to use or have access to NHS information

7.2 The Data Processor shall include appropriate confidentiality clauses in employment contracts, including details of sanctions against any employee acting in a deliberate or reckless manner that breaches confidentiality or the non-disclosure provisions of DPA or causes damage to or loss of NHS information.

7.3 The Data Processor shall ensure that all employees are aware of and act in accordance with the policies referred to in 6.1 above.

7.4 The Data Processor shall ensure that all employees are adequately trained to understand and comply with their responsibilities under DPA, the common law duty of confidence and this Agreement and shall provide the Data Controller with evidence of that training on request *or* as appendices to this Agreement.

7.5 Subject to clauses 7.1 – 7.4, the Data Processor shall ensure that only those employees involved in delivery of the contracted service use or have access to NHS information on a strict 'need to know' basis and shall implement appropriate access controls to ensure this requirement is satisfied.

7.6 The Data Processor shall ensure that any employees involved in delivery of the contracted service who do not specifically need to use personal information as part of their role have restricted access to anonymised NHS information and/or redacted extracts only.

8.0 Security – General

8.1 The Data Controller will not contract services from Data Processors unable or unwilling to comply with the terms of this Agreement and reserves the right to terminate the contract if either party is unable to agree necessary amendments in future.

8.2 The Data Processor shall not under any circumstances share, disclose or otherwise reveal NHS information (in whole or in part) to any individual, business or other organisation (3rd party) not directly involved in delivery of the contracted service without the explicit written consent of the Data Controller.

8.3 The Data Processor shall notify the Data Controller immediately of any untoward incidents or activities that suggest non-compliance with any of the terms of this Agreement. This includes 'near miss' situations even if no actual damage to or loss - or inappropriate disclosure of NHS information results.

8.4 The Data Processor shall indemnify the Data Controller against and compensate for any loss (financial or otherwise) that the Data Controller sustains due to any failure by the Data Processor or employees or sub-contractors to act in accordance with the terms of this Agreement and relevant legislation.

9.0 Security – Physical

9.1 The Data Processor shall ensure that all NHS information is physically protected from accidental or deliberate loss or destruction arising from environmental hazards such as fire or flood.

9.2 The Data Processor shall ensure that all NHS information is held on premises that are adequately protected from unauthorised entry and/or theft of NHS information or any IT equipment on which it is held by, for example, the use of burglar alarms, security doors, ram-proof pillars, controlled access systems, etc.

10.0 Security – IT Systems

10.1 The Data Processor shall hold electronically-based NHS information on secure servers unless otherwise agreed in writing.

10.1.1 NHS information will, under no circumstances, be stored on portable media or devices such as laptops, Tablet devices, smart phones (or any other portable computing equipment), or USB memory sticks or CD-ROM unless agreed in writing and subject, at a minimum, to those constraints detailed in section 10.2 and sub-sections.

10.2 The Data Processor shall ensure that:

10.2.1 All portable media used for storage or transit of NHS information are fully encrypted in accordance with NHS Guidelines on encryption to protect personal information.

10.2.2 Portable media are not left unattended at any time (e.g. in parked cars, in unlocked & unoccupied rooms, etc.).

10.2.3 When not in use, all portable media are stored in a locked area and issued only when required to authorised employees, with a record kept of issue and return.

10.3 The Data Processor shall not allow employees to hold NHS information on their own personal computers.

10.4 The Data Processor shall ensure adequate back-up facilities to minimise the risk of loss of or damage to NHS information and that a robust business continuity plan is in place in the event of restriction of service for any reason.

10.5 The Data Processor shall not transmit NHS information by email except as an attachment encrypted to 256 bit AES\Blowfish standards or from NHS mail to NHS mail.

10.6 The Data Processor shall only make printed paper copies of NHS information if this is essential for delivery of the contracted service.

10.7 The Data Processor shall store printed paper copies of NHS information in locked cabinets when not in use and shall not remove from premises unless this is essential for delivery of the contracted service.

10.8 The Data Processor shall provide the Data Controller Appropriate Assurance that it meets the requirements of the Data Protection Act 1998, and any NHS IG requirements deemed appropriate by the Data Controller.

11.0 Secure Destruction

11.1 The Data Processor shall ensure that NHS information held in paper form regardless of whether as 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.

11.2 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

11.3 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.

11.4 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.

12.0 Monitoring & Audit

12.1 The Data Processor shall permit the Data Controller to monitor compliance with the terms of this Agreement, by:

12.1.1 Allowing Data Controller employees or nominated representatives to enter any premises where NHS information is held, at all reasonable times and with or without prior notice, for the purpose of inspection.

12.1.2 Completing and returning a Data Processing Monitoring Form at the request of the Data Controller.

12.1.3 Provide independent assurance of the self-audited Information Governance Toolkit performance measures where the Data Processor is required to comply.

12.1.4 Staff will only review patients that are on their caseload. All systems are audited and any abuse or security breach in which data is compromised will be notified at the earliest opportunity via the Guardians of both Organisations and report the incident onto their incident reporting tool. Access to the system will be immediately withdrawn. Any inappropriate processing of patient data will be managed in accordance with the HSCIC IG SIRI (Serious Information Risk Incident) management process, and when appropriate risk scored, investigated and reported on the HSCIC IG Toolkit.

Both parties to this agreement will:

- Ensure that unauthorised staff and other individuals are prevented from gaining access to personal data
- Ensure visitors are received and supervised at all times in areas where personal data is stored
- Ensure that all computer systems that contain personal data are password protected on the type of data held, but ensure that only those who need to use the data have access. The level of security should depend on the type of data held, but ensure that only those who need to use the data have access.
- Not leave their workstation/PC signed on when they are not using it.
- Not disclose personal data to anyone other than the Data Subject unless the Data Subject's consent has been provided, or it is a registered disclosure, required by law, or permitted by a Data Protection Act 1998 exemption
- Not leave information on public display in any form

Methods of transfer
Shared data is transmitted across the NHS N3 network and is encrypted (scrambled) in transit.

13.0 Legal Jurisdiction

13.1 This Agreement is governed by and shall be interpreted in accordance with the law of England and Wales.

13.2 In the event of a dispute, the parties to this Agreement agree to attempt to resolve such issues according to NHS dispute resolution procedures. In the event that agreement cannot be reached, the parties agree that the courts of England and Wales shall have exclusive jurisdiction to hear the case .

13.3 Each partner will keep the Data Controller fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner, of any data obtained in connection with this agreement.

14.0 Relevant NHS Publications

14.1 A range of publications can be obtained from www.dh.gov.uk, www.nhsemployers.org and www.connectingforhealth.nhs.uk, including relevant NHS codes for NWCSU and standards. These cover areas including confidentiality, information security

management, employment check standards and records management. It is the responsibility of the Data Processor to ensure they are compliant with these standards.

15.0 Closure or termination of the agreement

15.1 Any partner organisation can suspend this agreement for 45 days if security has been seriously breached. This should be in writing and be evidenced.

Any suspension will be subject to a Risk Assessment and Resolution meeting, the panel of which will be made up of the signatories of this agreement, or their nominated representative. This meeting to take place within 14 days of any suspension.

Termination of this Data Sharing Agreement should be in writing to all other Partner Organisations giving at least 30 days' notice.

Signatories

Each partner should identify who is the most appropriate post holder within their agency to sign the agreement having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their organisation to the indemnity. In most cases it will be the organisation's Caldicott Guardian who will be signatory to data sharing agreements.

Signatories:

Name		Name	
Role		Role	
Organisation		Organisation	
Signature		Signature	
Date		Date	