**Data Sharing Agreement**

|  |  |
| --- | --- |
| 1. Name of Data Sharing Agreement: GP Information Sharing | |
| **Between:** | HCRG Care Group  and  GPs “Partner Organisation” |
| **HCRG Care Group Service:** | Adult Community Services |
| **Brief outline of agreement:** | To deliver health care to clients for direct care purposes and to allow data sharing of care records through EMIS for EMIS practices to increase the quality of care. This will be a two-way sharing initiative. |
| **Date of agreement:** | September 2022 |
| **Next date of review:** | September 2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Control** | | | |
| Date | Status | Reason for update | Reviewed by |
| 11/08/2020 | Draft | Draft for consideration by GP practices | V1.0 Antje Hirschmiller |
| 19/01/2021 | Version | Consideration of CCG comments | V1.1 Antje Hirschmiller |
| 31/03/2021 | Final Signed | Minor changes on request GP DPO, signatures, update of Records Management Code of Practice to 2020 version | V2.0 Antje Hirschmiller |
| 21/09/2022 | Update Version for signature | Rebranding to HCRG Care Group. Minor changes to signatures and update of Records Management Code of Practice to 2021 version | V3.0 Melissa Odawa |
| 17/01/2023 | Updated version for signature | Updated Appendix B Practice List. | V3.3 Alex Pearsall |

**Table of Contents**

**1.** Introduction3

1. Scope3
2. Definitions3
3. Data Sharing Agreement detail4
4. Key contacts14
5. General Obligations of all parties to this agreement15
6. Indemnity18
7. Review of agreement18
8. Termination and variation18
9. Dispute resolution19
10. Signatures19
11. Appendix A- Glossary and abbreviations21
12. Appendix B – List of GP Practices25
13. Appendix C – HCRG Care Group Communication26

# 

# Introduction

## This Data Sharing Agreement (‘the agreement’) is an overarching agreement to facilitate the exchange of data between the organisations party to it (‘parties’).

## All organisations involved in providing services to the public have a legal responsibility to ensure that their use of all person identifiable data (‘personal data’) is lawful, properly controlled and that an individual’s rights are respected.

## The agreement provides a framework for safeguarding the processing of personal data; however it is incumbent on parties to recognise that any data shared must be justified on the merits of each case.

## Adherence to this agreement does not provide any form of legal indemnity for any party from data protection legislation or any other law. It only serves to justify the data shared and to demonstrate that the parties have been mindful of and documented compliance with the relevant laws, nationally dictated organisational responsibilities and guidance.

## The agreement is not intended to replace local policy but to support it and provide guidance where none already exists. It should also be read in conjunction with the staff guidelines in place within each organisation regarding the transfer or sharing of personal data.

## The Caldicott Guardian or Senior Information Risk Owner (SIRO) must sign on behalf of each organisation. Where no such position exists, a Director or most senior person responsible for Data Protection requirements may act as signatory.

# Scope

## 2.1. The aim of this agreement is to ensure that the data sharing is appropriately covered in a straightforward and transparent manner.

## 2.2. The agreement applies to all persons working in or for the parties’ organisations (‘staff’) e.g. employees, volunteers, contractors, students, those employed via agencies, etc. who have access to the personal data on the system.

## 2.3. The parties must ensure this agreement is disseminated, understood, and acted upon by relevant staff, via training or other communicated means.

## 2.4. The parties must ensure that the specific department or team involved in the data sharing is clearly identified. Internal organisational access to shared data must be limited to those with a legitimate and approved need to see that data.

## 2.5. The agreement applies to all data processed under this agreement by the organisations, no matter in what format.

# Definitions

## 3.1 Data Protection Legislation: The UK General Data Protection Regulation (UK GDPR), the Data Protection Act (DPA) 2018 and the common law duty of confidence (confidentiality) all provide individuals with the right to privacy and confidentiality and the expectation that healthcare organisations will keep their data safe and secure.

## 3.2 Controller: A controller determines the purpose and means of processing personal data. Where engaging a processor, UK GDPR places further obligations to ensure contracts with processors comply with UK GDPR.

## 3.3 Processor: A processor is responsible for processing personal data on behalf of a controller. The UK GDPR places specific obligations on processors to maintain records of personal data and processing activities. Processors will also have legal liability if responsible for a breach.

## 3.4 Personal data: any data relating to an identifiable person who can be directly or indirectly identified in particular by a reference to an identifier. Pseudonymised data call fall within the scope of UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

## 3.5 Special categories of personal data: any data relating to an individuals’ race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

## 3.6 A glossary and list of abbreviations can be found in [Appendix A.](#_12._Appendix_A)

# Data Sharing Agreement detail

|  |  |
| --- | --- |
| **Party** |  |
| Party | HCRG Care Group |
| Data Protection Designation | Data Controller |
| Party | General Practices (for details see Appendix B) |
| Data Protection Designation | Data Controller |

|  |
| --- |
| **Purpose, objectives of the data sharing** |
| The information sharing agreement has been drafted to support clinicians in sharing relevant and appropriate clinical information between the GP practices and Adult Community services within HCRG Care Group for the purposes of Direct Care, using the EMIS clinical information system.  The GPs will sign up to the EMIS Configuration document which will be managed by the HCRG Care Group clinical systems team who will then complete the technical information sharing.  The purpose of the sharing of information detailed in this agreement is:  1. To deliver health care to patients  2. Support services that are managed by HCRG Care Group & GP practices  3. To allow appropriate data sharing of care records through EMIS to EMIS |

|  |
| --- |
| **Benefits of the data sharing** |
| * Access to patient details at the point of care * Time saving for the patient and clinical staff at both the GP practice and the HCRG Care Group services * Medical accuracy regarding medication reviews and patient history |

|  |
| --- |
| **Data Privacy Impact Assessment** |
| A DPIA has been completed by HCRG Care Group |

|  |
| --- |
| **Lawful basis for processing the data** |
| Personal data can be processed and shared providing the processing and sharing complies with the Data Protection Legislation. |
| **Sharing for Direct Care Purposes** Where sharing is for the purpose of delivery of direct care or administration (waiting list management, performance against national targets, activity monitoring, local clinical audit, production of datasets to submit for commissioning purposes and national collections), UK GDPR Article 6(1)e and 9(2)(h) is the most appropriate lawful basis.  These conditions will also apply where an organisation participates in activities with a statutory basis, such as responding to a public health emergency. |
| * **Article 6(1)(e)** – ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority’.   Where special categories personal data is being processed for purposes related to the commissioning and provision of health and social care services the condition is:  **Article 9(2)(h)** – ‘processing is necessary for the purposes of preventive or occupational medicine, for ... medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services...’ |

|  |  |
| --- | --- |
| **UK GDPR Article 6(1)(e) and Article 9(2)(h) is the lawful basis** | Yes |
| **Sharing for Safeguarding Purposes** For the purposes of safeguarding vulnerable patients/service users, the Article 6(1)(e) and 9(2)(b) may apply.  The Children Act 1989 (CA) establishes implied powers for local authorities to share information to safeguard children. Local authorities have a duty to investigate where a child is the subject of an emergency protection order, is in police protection or where there is reasonable cause to suspect that a child is suffering or is likely to suffer significant harm. The CA also requires local authorities ‘to safeguard and promote the welfare of children within their area who are in need’ and to request help from specified authorities including NHS organisation. These are required by the CA to comply ‘…with the request if it is compatible with their own statutory or other duties and obligations and does not unduly prejudice the discharge of any of their functions’. Under the Children Act 2004 local authorities must make arrangements to promote cooperation with relevant partners and others, to improve well-being. |  |
| * **Article 6(1)e** – ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority’.   Where special categories personal data is being processed for purposes related to the commissioning and provision of health and social care services the condition is: |  |
| **Article 9(2)(b) –** ‘‘…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law...’ |  |
| **UK GDPR Article 6(1)(e) and Article 9(2)(b) is the lawful basis** | Yes |

|  |  |
| --- | --- |
| Explicit consent is available as a lawful basis for processing special categories of data but is not normally use consent as a legal basis in a healthcare setting. |  |
| **Consent is the lawful basis** | **No** |

|  |  |  |
| --- | --- | --- |
| **Data items to be processed** |  |  |
| Data item | Justification | Lawful basis |
| Demographic Information:   * Full name * Full date of birth * Full postal address (including full postcode) * Telephone number (including area code) * Mobile number * Email address * Hospital Number   NHS Number | To support Direct Care of the patients | UK GDPR Article 6(1)(e) and Article 9(2)(h)  UK GDPR Article 6(1)e and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care),  Common Law Duty of Confidentiality |
| Care Record Summary | To support Direct Care of the patients | UK GDPR Article 6(1)(e) and Article 9(2)(h)  UK GDPR Article 6(1)e and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care),  Common Law Duty of Confidentiality |
| Consultations | To support Direct Care of the patients | UK GDPR Article 6(1)(e) and Article 9(2)(h)  UK GDPR Article 6(1)e and Article 9(2)(b)  Duty of Confidentiality |
| Medication | To support Direct Care of the patients | UK GDPR Article 6(1)(e) and Article 9(2)(h)  UK GDPR Article 6(1)(e) and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care)  Common Law Duty of Confidentiality |
| Problems | To support Direct Care of the patients | UK GDPR Article 6(1)(e) and Article 9(2)(h)  UK GDPR Article 6(1) (e) and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care)  Common Law Duty of Confidentiality |
| Investigations | To support Direct Care of the patients | UK GDPR Article 6(1) (e) and Article 9(2)(h)  UK GDPR Article 6(1) (e) and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care)  Common Law Duty of Confidentiality |
| History | To support Direct Care of the patients | UK GDPR Article 6(1) (e) and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care)  Common Law Duty of Confidentiality |

|  |  |  |
| --- | --- | --- |
| Diary and Appointments | To support Direct Care of the patients | UK GDPR Article 6(1)(e) and Article 9(2)(h)  UK GDPR Article 6(1) (e) and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care)  Common Law Duty of Confidentiality |
| Attachment’s | To support Direct Care of the patients | UK GDPR Article 6(1)(e) and Article 9(2)(h)  UK GDPR Article 6(1) (e) and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care)  Common Law Duty of Confidentiality |
| Referrals | To support Direct Care of the patients | UK GDPR Article 6(1)(e) and Article 9(2)(h)  UK GDPR Article 6(1) (e) and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care)  Common Law Duty of Confidentiality |
| Safeguarding | To support Direct Care of the patients and any known safeguarding concerns of patients | UK GDPR Article 6(1)(e) and Article 9(2)(b) and (h)  UK GDPR Article 6(1) (e) and Article 9(2)(b)  Health & Social Care Act 2015 (Direct Care)  Common Law Duty of Confidentiality |

|  |  |
| --- | --- |
| **Data Sharing** |  |
| Who will share the data | The GPs and HCRG Care Group will be sharing the data. |
| How will the data sharing be carried out | EMIS System Access |
| Who in each organisation will have responsibility for overseeing the Processing | The GPs and the HCRG Care Group Services will have responsibility for overseeing the processing. |
| How is the data secured and who is responsible for ensuring security | Role Based Access Controls  Audit Transaction Monitoring will be in place  HSCN secure accredited area  Under no circumstances should personal data be processed in any way that is unsecure or left unattended. It is the responsibility of the sender to ensure that the method is secure and that they have the correct contact details for the receiver. |
| Is any data to be transferred outside the EEA | No |
| What record will be kept of what has been shared with whom | All information will be recorded on the patient’s health record on the EMIS system which will be regularly monitored and reviewed. |

|  |  |
| --- | --- |
| **Data Quality Detail** |  |
| How will data quality be managed; What is the process for ensuring omissions, errors, etc are corrected | Each individual user will be responsible for ensuring the accuracy of their data in the EMIS system. The HCRG Care Group managers for the service will carry out regular access audits and auditing the data for data quality purposes in accordance with its policy and procedures and in order to comply with legislation, best practice, and the NHS Digital DSP Toolkit requirements. |
| Who will carry out the auditing | HCRG Care Group Clinical Systems Team and the GPs |
| Who is responsible for corrections | HCRG Care Group Clinical Systems Team and the GPs |
| What is the escalation procedure for problems | If there are any issues, then the relevant GP must notify HCRG Care Group without delay. |

|  |  |
| --- | --- |
| **Privacy Notice** |  |
| Who will advise data subjects about the processing carried out as a result of the data sharing covered by this agreement | HCRG Care Group and the GPs will each ensure they have a privacy notice in place that will be specific to the service. This will be made publicly available both in manual and electronic forms. |
| How will this be communicated | Verbally and electronically |
| If you are processing any personal data about children, what have you done to ensure that your privacy notice is accessible to them | Privacy notices will be available on the HCRG Care Group Website. |
| Where joint controllership applies, has this been made clear in the privacy notice | N/A |

|  |  |
| --- | --- |
| **Individual’s Rights** |  |
| Has a contact point for data subjects been indicated in the privacy notice | Privacy notices will be available on the HCRG Care Group Website. |
| What is the process to keep the other party up to date about amendment, erasure, or restriction of use of data shared under this agreement | HCRG Care Group will be responsible for any information requests as Data Controller, and these will be documented within the HCRG Care Group privacy notice.  **Important message to be shared with all relevant HCRG Care Group and GP Surgery staff:**  **Each party will agree to only disclose information under a Data Subject Access Request which they control.**  **Having access to the Partner Organisation Health Care Record does not allow the other party to disclose this information should they receive a request for the information (unless this has been shared with them to form part of their records (e.g. referral letters cc’d to them, discharge summaries sent to them, etc). Any requests received concerning data which is accessible but controlled by the Partner Organisation must be directed to the source of the data without delay.** |

|  |  |
| --- | --- |
| **Records Management Detail** |  |
| Is the data to be processed in paper | No |
| If yes, who will hold the paper data | N/A |
| If yes, how will the paper data be stored | N/A |
| How will the paper data be returned or destroyed | N/A |

|  |  |
| --- | --- |
| **Shared system** |  |
| What is the name of the system(s) | EMIS |
| Access control detail | Role based access control  Smart Card access |
| What is required prior to a User being given access | Users to ensure they have been trained on the system.  Sign and agree the acceptable use agreement where applicable.  Completed their IG training within the same financial year. |
| Who will sign off the access to be given (HCRG Care Group only) | Senior Service Manager (following the appropriate Starters/Movers/Leavers process which includes notification of the Clinical System’s Team and other relevant IAO’s. |
| Department and/or person who will give the User access to the data | Clinical Systems Team (HCRG Care Group) |
| How will access be given | Access will be given by username and password |
| Name of the person maintaining the list of Users and informing when a User no longer requires access (HCRG Care Group only) | Anne Crozier – Clinical Systems Lead |
| What is the procedure for terminating User access | Access will be terminated via the clinical systems team – HCRG Care Group (Starters/Movers/Leavers process) |
| Department and/or person responsible for terminating access | Clinical Systems Team – HCRG Care Group |
| How will monitoring access to the data take place | Monitoring will be by regular reporting and on demand reporting where requested by an appropriately senior member of staff – HCRG Care Group.  Annual Health Care Record Audit.  On request investigations by the Clinical System’s team.  Cross checking against starter/mover/leaver data. |
| Who will carry out the monitoring | The Controller will monitor access in accordance with its policy and procedures |
| What is the escalation procedure for problems relating to access to the data | Problems relating to inappropriate access will be escalated to the Caldicott Guardian and/or the Head of Information Governance and/or local IG Lead and the Information Asset Owner (IAO) for the system. |

|  |  |
| --- | --- |
| **Retention Periods** |  |
| How long will the data be retained for | All data, whether held on paper or in electronic format must be stored and disposed of in line with each partner organisation’s retention and disposal schedule. Retention periods should be informed by the [Records Management Code of Practice](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/) published on 4 August 2021 by the Information Governance Alliance (IGA). |
| Disposal of data | The disposal of confidential data in paper or digital format will be carried out in line with each organisation’s policy which must comply with the NHS Digital [Disposal of Confidential Data Guidance.](http://systems.digital.nhs.uk/infogov/security/infrasec/gpg/dadosd.pdf) This should include provision for notification of such deletion/destruction. |

|  |  |
| --- | --- |
| **Management of the Agreement** |  |
| Who will keep signed copies of the agreement | The Head of Information Governance or person responsible for Data Protection at each Party will retain copies of the Agreement. |
| Review of the agreement | The agreement will be reviewed annually for effectiveness unless the parties become, or are made, aware of reasons for an earlier review. |
| Who will undertake the review of the agreement and agree any changes | The Caldicott Guardian or person responsible for Data Protection and/or the Head of Information Governance at each Party will undertake the review and agree any changes |
| Who will pay for associated costs of any review | Costs will be borne equally by the parties |
| Can this agreement be shared as part of the publication scheme of the organisation (if relevant) | n/a |
| How will the agreement be terminated | This agreement will be terminated by agreement of the parties or by non-compliance. |

# Key Contacts

|  |  |
| --- | --- |
| **Key Contacts of HCRG Care Group** |  |
| Senior Information Risk Owner (SIRO) | David Deitz |
| HCRG Care Group Caldicott Guardian | David Watkins |
| Head of Information Governance (Interim) | David Watkins |
| Local IG Lead | Jamie Maslen |
| Deputy Caldicott Guardian, North Kent | Amanda Caldicott |
| Information Asset Owner | Anne Crozier |
| Sponsor | Matt Tizora |
| Clinical Systems Manager (where relevant) | Alex Pearsall |

|  |  |
| --- | --- |
| **Key Contacts Partner Organisation** |  |
| Senior Information Risk Owner (SIRO) | xx |
| Caldicott Guardian | xx |
| Head of Information Governance | xx |
| Information Asset Owner (where relevant) | xx |
| Other contact(s) e.g. IT contact, service/department contact, etc. | xx |

# General Obligations of all parties to this agreement

## 6.1 This agreement must be agreed by all parties to be in force.

## 6.2 The parties agree to be responsible for ensuring full compliance of all staff within their organisation to the terms and conditions of this agreement.

## 6.3 All parties in this agreement will comply with the following general obligations:

|  |  |
| --- | --- |
| **General Obligations** |  |
| ICO | Be registered with the UK information Commissioner to carry out data processing activities and keep up to date its registration with the Information Commissioner |
| IG Toolkit | Each party shall Maintain Level 2 in the requirements of the Data Security and Protection Toolkit (DSPT) relevant to their Processor type, to include:   * Cyber Essentials * IG training by all staff accessing personal data to be up to date |
| Data Controller arrangements | Be responsible for the data they hold and process (once safely received) from the other party as data controller of that information |
| Data sharing oversight | Have appointed and named a responsible officer who will ensure the protection of personal data, e.g. Caldicott Guardian or senior manager responsible for data protection |
| Legal Compliance | Comply with its obligations under data protection legislation, policies, and standards and under the common law duty of confidentiality |
| Lawfulness, fairness, and transparency | Comply with ‘The right to be informed’, and ensure that details of any new processing/sharing will provided to the data subjects and be accurate, transparent, and informative, and suitable for the intended audience |
| Purpose limitation | The data will only be processed by staff in order for them to perform their duties for the purposes identified and not processed for any other purposes. The core purpose is the provision of health and social care services, further processing of the data, such as managing and planning services, cannot be undertaken without the approval of all partners. |
| Data minimisation | Process only data, which is adequate, relevant, and limited to what is necessary |
| Accuracy | Take all reasonable steps to ensure data processed is correct.  All parties are responsible for informing any source partner of any accuracy issues they identify within the data shared. Any data quality issues that may significantly affect the care of an individual will be reported to relevant partners immediately (i.e. any issue that may either delay provision of care or risk the effectiveness of care). Issues that are not critical, such as a potential misinterpretation of data should be reported so that issues can be assessed and addressed. |
| Storage limitation | Will not keep personal data for longer than it is need for the purposes identified |
| Integrity and confidentiality | Agree to treat the data received under the terms of this agreement as confidential and safeguard it accordingly and respect the privacy of individuals at all stages of processing.  All parties, whether they are providing or just viewing data, are responsible for implementing appropriate technical and organisational measures to ensure the security of the data within any shared system. |

|  |  |
| --- | --- |
| Accountability | Be responsible for, and be able to demonstrate, compliance with the data protection principles. |
| Overseas Processing | Before information can be processed outside of the UK all parties must be informed of this intent with sufficient notice in writing. Information will not be processed outside of the European Economic Area without the appropriate safeguards being in place. |
| Complaints, queries, and objections | Notify the other parties to this agreement of any complaint received from any person about the sharing of data under this agreement or any correspondence from the Information Commissioner or other regulator regarding the sharing of data under this agreement.  Assist each other in responding to requests made under the Freedom of Information Act 2000 or Environmental Information Regulations 2004 in relation to the data shared under this agreement to ensure a co-ordinated and consistent response unless an exemption under the Act applies.  Where information is held jointly, it is the responsibility of the organisation receiving the request to ensure they request promptly all relevant information from the other parties.  Where one party receives a request meant for the other, such requests will be sent to the other party immediately and safe receipt confirmed. |
| Breach | Information breaches will be the responsibility of the party in which the breach occurred. All breaches should be assessed in line with the ‘Guide to Notification of Data Security and Protection Incidents’ (<https://www.dsptoolkit.nhs.uk/Help/29>). This provides a common tool for scoring of incidents, noting when an incident should be reported to the Information Commissioner’s Office and affected individuals.  Where a party identifies a reportable breach, it should inform any other parties within 24 hours.  A breach that is not classed as reportable will be managed by the partner identified as responsible and will engage other parties as required. |
| Use of third parties (processors) | The parties to this agreement will not instruct further processing of the shared data by any third parties without the consent in writing of the partner organisations. |

# Indemnity

## 7.1. Each party shall indemnify the other against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other [reasonable] professional costs and expenses) suffered or incurred by the indemnified party arising out of or in connection with the breach of the Data Protection Legislation by the indemnifying party, its employees or agents, provided that the indemnified party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it.

# Review of agreement

## 8.1. The data sharing and this agreement will be reviewed by a suitably qualified individual or committee/group within each organisation every two years and/or if changes to the legislation apply on an ad hoc basis as and when required. This agreement will remain in force irrespective of whether the agreement has been officially reviewed until a notice of termination is served.

# Termination and variation

## 9.1. Any partner organisation may leave this agreement by giving thirty calendar (30) days’ notice in writing to HCRG Care Group.

## 9.2. Any proposed changes to the parties involved in this agreement, to the purposes of the data sharing, the nature or type of data shared or manner in which the data is to be processed and any other suggested changes to the terms of this agreement must be notified immediately to the relevant Information Compliance/Governance leads so that the impact of the proposed changes can be assessed.

## 9.3. No variation of the agreement shall be effective unless the agreement is amended, and it is signed by all parties.

## 9.4. Each party will abide by the provisions of this agreement until such time as the processing of the personal data ceases. However the terms of this agreement remain binding in respect of any data shared and retained throughout its lifecycle, irrespective of whether the party remains a current signatory to this agreement.

## 9.5. On termination of this agreement any rights, remedies, obligations, or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of this agreement which existed at or before the date of termination, shall not be affected.

# Dispute and resolution

## 10.1. In the event of a dispute arising under this agreement, authorised representatives of the parties will discuss and meet as appropriate to try to resolve the dispute within seven calendar (7) days of being requested in writing by any party to do so. If the dispute remains unsolved, it will then be referred to a senior manager from each of the parties who will use all reasonable endeavours to resolve the dispute within a further fourteen calendar (14) days.

## 10.2. In the event of failure to resolve the dispute through the steps set out above the parties agree to attempt to settle it by mediation.

# Signatures

We agree to give view access to the following information through EMIS for named Clinicians within authorised organisations in accordance with the sharing agreement.

**GP’s and Adult Community Services provided by HCRG Care Group access to:**

* Demographic Information
* Care Record Summary
* Consultations
* Medication
* Problems
* Investigations
* History
* Diary and Appointments
* Attachments
* Referrals

Signed for and on behalf of:

|  |
| --- |
| Organisation: HCRG Care Group |
| Name: Amanda Caldicott |
| Position: Deputy Caldicott Guardian |
| DPA Registration No.: Z2823541 Date of expiry/re-registration: 23 August 2023 |
| Signature: ***A.Caldicott*** |
| Date: 04/10/2022 |

Signed for on behalf of:

|  |  |
| --- | --- |
| Partner Organisation: Name of Practice: xx |  |
| Name of Practice Manager or GP Lead | xx |
| Contact Details e.g. Address and direct email address | xx |
| Practice Code / NACS Number | xx |
| CDB Number (EMIS System Number) | xx |
| DPA Registration No: xx | Date of expiry/re-registration: xx |
| Signature: xx |  |
| Date: xx |  |

# 12. Appendix A - Glossary and abbreviations

|  |  |
| --- | --- |
| Caldicott Guardian | A senior person responsible for protecting the confidentiality of patient and service-user data and enabling appropriate data-sharing. |
| Consent forms | Consent forms are forms that are used to obtain the permission of the data subject for their personal data to be used for a particular purpose. A consent form can be used at the point of collection (as part of the collection text) or later if the particular purpose was not explicitly mentioned when the data was collected.  Specific conditions must be met when using consent as a legal basis. These should be documented within the DPIA. |
| Data | “Data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. |
| Data Controller | A Data Controller determines the purposes and means of processing personal data.  Each legal entity within HCRG Care Group will be a Controller or a Processor as identified in the health care contract. |
| Data Controller - Joint | Joint controllers are two or more controllers that jointly determine the purposes and means of processing. No matter what the arrangement is between the joint controllers, the data subject may exercise his or her rights in respect of and against each of the controllers.  Data Controllers in Common is not a concept under new data protection legislation. |
| Data Processing | Data Processing means any manual or automated actions in relation to the data.  Actions includes collection, recording, storage, alteration, retrieval, use, disclosure by transmission, blocking, erasure and destruction. There must be a lawful basis for processing personal and special category data and any processing must comply with the data protection principles. |
| Data Processor | A Data Processor is responsible for processing personal data on behalf of a controller. Under new data protection legislation a data processor has a number of obligations.  Data processors as well as data controllers are liable to data subjects for breaches.  Each legal entity within HCRG Care Group will be a Controller or a Processor as identified in the health care contract. |
| Data Subject | A Data Subject is the individual who is either the direct subject of the personal data or can be identified from it.  Data subjects have the right to compensation from a data controller or data processor. |
| Data: Personal data | Information which has been gathered by the controller or processor relating to a living individual which identifies them.  Personal data can include pseudonymised data depending on how difficult it is to attribute the pseudonym to a particular individual. |
| Data: Special Category data | Data concerning health is classed as special category data and requires additional conditions and safeguards.  The inclusion of genetic and biometric data as sensitive personal data is new and will need to be reflected in policy and contracts. |
| Data: Anonymised | Data protection legislation does not apply to data that is fully anonymised in such a way that individuals cannot be identified. |
| Data: Pseudonymised | Pseudonymised data will be treated as personal data because individuals can potentially be identified, albeit via a key. |
| Deceased individual | The Access to Health Records Act (AHRA) 1990 provides certain individuals with a right of access to the health records of a deceased service user. These individuals are defined under the Act as, ‘the service user’s personal representative and any person who may have a claim arising out of the service user’s death’. A personal representative is the executor or administrator of the deceased person’s estate. |

|  |  |
| --- | --- |
| Health and/or Care Record | A record which consists of data relating to the physical or mental health and/or social care of an individual |
| Privacy Notice | Privacy notices are to inform the person from whom personal data is being collected, the data subject, how data is going to be processed. Specific information must be provide to the data subject. |
| Publication schemes (Freedom of Information Act) | The Freedom of Information Act places a duty on public authorities to adopt and maintain a publication scheme that must be approved by the Information Commissioner. |
| Senior Information Risk Owner (SIRO) | The SIRO is an executive who is familiar with and takes ownership of the organisation’s information risk policy and who acts as advocate for information risk. |
| Subject Access Request for living individual | A subject access request (SAR) is a request received from an individual asking to provide them with copies of the data held about them. Individuals have the right to access data held about them under the Data Protection Act 2018 (DPA). |
| Third Party | A person or organisation other than the data subject or HCRG Care Group. |
| DPA | Data Protection Act. The DPA 2018 sets out the framework for data protection law in the UK. It sits alongside the UK General Data Protection Regulation (GDPR), and tailors how the GDPR applies in the UK - for example by providing exemptions. |
| DPIA | Data Protection Impact Assessment. The DPIA is one of the specific processes mandated by the GDPR. Organisations must carry out a DPIA where a planned or existing processing operation – “is likely to result in a high risk to the rights and freedoms of individuals”. |

|  |  |
| --- | --- |
| DPO | Data Protection Officer. The UK GDPR makes it a requirement that organisations appoint a DPO in some circumstances. |
| DSPT | Data Security and Protection Toolkit (replaces the IG Toolkit from April 2018) |
| GDPR | The General Data Protection Regulation. UK GDPR came into force on May 25, 2018 and is designed to modernise laws that protect the personal data of individuals. It also boosts the rights of individuals and gives them more control over their data. |
| ICO | The Information Commissioner’s Office is a UK independent supervisory authority. It enforces and oversees the Data Protection legislation and the Freedom of Information Act 2000. |
| IG | Information Governance. |
| IGA | The Information Governance Alliance; the authoritative source of advice and guidance about the rules on using and sharing data in health and care. |

**13. Appendix B - List of GP Practices**

|  |  |
| --- | --- |
| **ODS code** | **DGS PRACTICES** |
| G82048 | Horsmans Place Surgery |
| G82185 | DARTFORD WEST HEALTH CENTRE/Redwood Practice |
| G82647 | Temple Hill Group |
| G82006 | Dartford East Health Centre (formerly Dr Shimmins) |
| G82143 | Lowfield Street |
| G82122 | Swanscombe Health Centre |
| G82212 | Pilgrims Way Partnership |
| G82809 | Downs Way Medical Practice |
| G82044 | Springhead Health Ltd |
| G82808 | Oakfield Health Centre |
| G82032 | Pelham Medical Centre |
| G82648 | Rochester Road Surgery |
| G82780 | Gravesend Medical Centre |
| G82073 | Meopham Medical Practice |
| G82097 | Jubilee Medical Group |
| G82028 | The Cedars Surgery |
| G82088 | Devon Road Surgery |
| G82218 | Farningham (Braeside Surgery) |
| G82225 | THE OAKS PARTNERSHIP/The Oaks Surgery |
| G82056 | THE ORCHARD PRACTICE used to be The Wellcome Practice |
| G82062 | Parrock Street Surgery |
| G82021 | The Shrubbery & Riverview Park Surgery |
| G82067 | Old Road West Surgery |

|  |  |
| --- | --- |
| **ODS code** | **SWALE PRACTICES** |
| G82023 | Sheerness Health Centre (Dr Patel) |
| G82057 | St George’s Medical Centre and branches |
| G82682 | The OM Medical Centre |
| G82687 | VEL Surgery |
| G82799 | Sheppey Healthy Living Centre |
| G82035 | The Chestnuts Surgery |
| G82231 | London Road Medical Centre |
| G82693 | The Memorial Medical Centre |
| G82698 | The Medic Care Surgery |
| G82026 | Grovehurst Surgery |
| G82634 | The Meads Medical Practice |
| G82702 | Green Porch Medical Partnership |
| G827410 | Princes park |