The Royal Marsden NHS
NHS Foundation Trust

203 Fulham Road, London, SW3 6JJ
Telephone: 020 7811 8217

INFORMATION SHARING AGREEMENT

Coordinate My Care

SCOPE	Coordinate My Care
NAME OF LEAD	Prof. Julia Riley
APPLIES TO	NHS and non-NHS organisations involved in patient care
RELATED DOCUMENTS	CMC IG Pathway Overview CMC Participating Organisations List System Level Security Policy Privacy Impact Assessment Business Continuity Plan User Access Form Acceptable Use Policy Patient Information Leaflet Mobile Device Operational and Support Policy CMC Automated Flagging How-To Guide
VERSION	Version 4.8 dated 17.10.2018
MONITORING & REVIEW PROCESS Please describe the monitoring and review process for this particular Agreement; include reference as to who will be involved and how any ad-hoc actions (e.g. queries, complaints etc.) will be handled.	Annual review

TABLE OF CONTENTS

Version Control

Version Number	Amendments made	Changes made by	Date
2.0	• **Section 3.1** to clarify consent for patients that lack mental capacity • **Section 4.7** added to outline the action required if and when CMC programme terminates	Information Governance Manager, The Royal Marsden	6th November 2012
3.1	• **Section 4.8** repetition of the word provider removed • **Page 13 signature page** duplicate signature box deleted • **Page 13** following sentence added "An up to date list of participating organisations may be obtained from the Coordinate My Care Team upon request"	Information Governance Administrator, The Royal Marsden	10th December 2012
3.3	• **3.1 and 5.5** replace 'anonymised' by 'pseudonymised' • **4.4** remove 'the information contains medical details' • **4.10** 'Information will of course be made available to signatories of this agreement during the retention period.'	CMC IT Architect	16th January 2013

Version Number	Amendments made	Changes made by	Date
3.4	• **2.1 and 3.1** additional CMC background information • **3.1** Clarification re explicit consent/MCA 2005 • **4.3** Remove reference to 'confidential reference' • **5.2** Remove second bullet point (not relevant to CMC) • **5.2** Remove last two bullet points (information covered more clearly elsewhere in document) • **5.4** Corrected to reflect CMC environment more accurately • Minor formatting and typo corrections	CMC Development Manager and CMC IT Architect	17th January 2013
3.5	• **3.1** Clarify Social Services information shared • **4.2** Add additional information re requirements of DPA 1998 as specifically relevant to CMC's processing of personal sensitive information • **4.4** Change 21 days to 40 days	CMC IT Architect	28th January 2013
3.6	• **5.5** Clarification re retention and disposal of CMC data	CMC IT Architect	6th February 2013

Version Number	Amendments made	Changes made by	Date
3.7	• Minor formatting improvements & typo corrections • Extend Related Documents list on title page • 1.2 Clarify 'specified organisations' by referring to Summary of Endorsements page • **3.1** Make it clear that receipt of consent is explicitly recorded on the CMC System • **4.3** Clarify last paragraph • **4.6** Refer to section 3.1 re consent • **4.8** Additional bullet point re informing original data controller of details and outcome of investigation • **4.9** Specific reference to DPA 1998 • **5.1** Clarify that the PIA is made available to CMC user organisations alongside the ISA • **5.3** Add reference to CMC Legitimate Relationships handling • **5.4** Remove content not relevant to CMC, for clarity • **Appendix A** Add 'The NHS Act 2006 (section 251)' and 'The NHS Records Management Code of Practice', remove 'The Health and Social Care Act 2001 (Section 60)' and 'The Civil Contingencies Act (2004) Part 1 and supporting regulations'	CMC IT Architect	18th June 2013
3.8	• **1.3** and **1.4** Rephrased • **3.2** Section Added • **Summary of Endorsements** Note added re signature of ISA at CCG rather than GP practice level in some cases	CMC IT Architect	25th September 2013

Version Number	Amendments made	Changes made by	Date
4.0	• Remove all references to London • Coverage on title page of non-NHS organisation usage of CMC • CMC-specific IG Toolkit added to Related Documents on title page • **1.3** and **1.4** Minor amendments for clarity • **3.1** Clarification of Information to be Shared, and of information sharing for research purposes; allow for access by nursing home staff and social workers • **4.3** Handle situation where no Caldicott Guardian • **5.2** Remove reference to NHS and clarify that all CMC user organisations must be covered by an IG Toolkit, whether NHS or not • **5.3** User IG training mandate of IG Toolkit applies to all CMC users, whether NHS or not • **5.4** Updated in detail to reflect current situation • **5.5** Royal Marsden data retention policy now implemented for CMC; records can also be removed completely if specific circumstances mandate this	CMC IT Architect	13th February 2014
4.1	• Add new CMC IG Pathway Overview to Related Documents list on title page • **5.3** Change CRB to Disclosure and Barring Service (DBS)	CMC IT Architect	22nd May 2014

Version Number	Amendments made	Changes made by	Date
4.2	• **2.1** Add 2 paragraphs at top of text box to provide brief description of CMC service. • **4.1** Reflect Caldicott 2. • **5.3** Generalise to 'health or social care professional'. • **5.4** Update to reflect current information flows. • **Summary of Endorsements** Note removed re signature of ISA at CCG rather than GP practice level in some cases. Additional input boxes provided, for greater clarity re signatory and re organisations represented. Royal Marsden signature dated. ISA version added to footer.	CMC IT Architect	1st December 2014
4.3	• Title page updated to identify current CMC General Manager and to remove reference to obsolete Out of Hours S.O.P., also final reference to London. • **3.1** Clarify situation re Disease Specific Care Plans from 24.11.2015. • **5.3** Allow for electronic confirmation by user of agreement to Acceptable Use Policy. • **5.4** Update to reflect data flow changes relating to the upcoming migration of the CMC System to a new platform/managed service (24.11.2015).	CMC IT Architect	2nd November 2015
4.4	• **5.4** Update data flows to reflect EMIS Web in-context link & CMC Availability Service; indicate that 24.11.15 migration and Demographics Changes Reports data flows are obsolete. • Replace 'Personalised Care Plan' by 'Urgent Care Plan'. • Except re migration data flow, remove all references to 24.11.2015 and to System C/Liquidlogic.	CMC IT Architect	4th May 2016
4.5, 4.6	• **4.2 and Appendix A** Add references to Health and Social Care Act 2012, re Duty to Share Information	CMC IT Architect	5th, 13th July 2016

Version Number	Amendments made	Changes made by	Date
4.7	• **2.1** Add reference to Patient Portal. • **4.10** Clarify situation should a particular locality discontinue use of CMC. • **5.3** Clarify situation re implicit declaration of Legitimate Relationship on care plan publication. • **5.4** Document the secure logging of Availability Service calls by CMC's Managed Service provider. • **5.4** Document use by 111 of CLI (Telephone Number) Extract service & of Crisis Care Extract service.	CMC IT Architect	24th September 2016

Version Number	Amendments made	Changes made by	Date
4.8	• Related Documents listed on page 1 – removal of the CMC mini-IG toolkit as no longer available or required to support nursing home IG compliance. • Version Control moved to the end of the document • 3.1 Further information regarding engaging the Health & Welfare Lasting Power of Attorney in the context of the patient's lack of mental capacity to consent to a CMC care plan and a note on best practice where an appropriate LPA does not exists. • 4.2 Principles of Data Protection in section 4.2 adjusted to reflect fewer principles in number (from 8 to 6) in the DPA 2018 Act. • 4.2 Addition of the GDPR principles. • 4.3 Addition of GDPR stipulations as it relates to consent. • 4.3 The phrase 'non-care' is explained as research and service development. • 4.5 Addition of GDPR stipulations in relation to Breach of Confidentiality. • References to the Data Protection Act 1998 replaced with references to the Data Protection Act 2018 throughout the document (1.1,3.2,4.4 & Appendix 1) • References to the GDPR principles/obligations added throughout the document where applicable and where previously there was a reference to the Data Protection Act 1998 only. (1.1,3.2,4.4, 4.9 & Appendix 1) • 5.2 & 5.3 References to the HSCIC IG toolkit updated to NHS Digital Data Security and Protection Toolkit. • 5.5 Information added regarding the meaning of 'soft delete'.	CMC Director of Nursing and Royal Marsden Information Governance Manager	17th October 2018

1. INTRODUCTION

1.1. The parties to the agreement recognise that organisations need to work closely together in order to provide integrated services to patients. The exchange of information facilitates this partnership and must always adhere to legal requirements such as the Data Protection Act 2018 and the General Data Protection Regulation.

1.2. The purpose of this agreement is to formalise the data sharing arrangement between the specified organisations (see Summary of Endorsements within this document), whilst outlining the agreement's compliance against Information Governance standards.

1.3. Each organisation that supplies patient information to the CMC platform is the Data Controller of that information. However together the participating organisations are joint Data Controllers of all patient data shared via the CMC platform. This agreement sets out the allocation of responsibilities between participating organisations as Data Controllers.

1.4. By signing this agreement, each partner organization agrees that all other partner organisations may access, amend and manage information relating to its patients, in line with the terms of this agreement.

2. WHY IS THE INFORMATION BEING SHARED?

2.1. Please describe the reason(s) and specific purpose(s) for the sharing of service user information between the signatory organisations; include reference as to how the sharing of personal information will benefit the service users concerned and how each organisation will subsequently use the information.

Coordinate My Care (CMC) is an NHS initiative, run by The Royal Marsden NHS Foundation Trust and in place since August 2010, permitting the key information about an individual and their preferences for care (an Urgent Care Plan) to be recorded and accessed by a range of NHS and non-NHS service providers, and by patients and carers.

Non-urgent care providers collaborate to establish, maintain, and use the Urgent Care Plans of their patients. Urgent care providers are notified by CMC of the existence of Plans for specific patients/at specific addresses in their area. They can then identify the existence of a Plan for the patient at the time of call-out, and access this Plan in order to provide appropriate care.

CMC is a single solution to share information that has many advantages for patients:

- The information recorded on CMC relates to the current and advance care needs and plans of patients who have been identified as end of life or who have complex ongoing health needs (Heart Failure, Chronic Pulmonary Airways disease, Dementia).
- Wherever the patient is, assuming CMC coverage, the same record will be accessed, e.g. if patient goes to stay with a relative
- In any area of CMC coverage, all health and social care professionals know where and how to access CMC
- Doctors, nurses and social workers can move from one area to another and not have to retrain on another system
- Information is available 24/7 and can be accessed from anywhere to ensure patient-centric care is delivered at the right time, in the right place as quickly as possible

3. WHAT IS TO BE SHARED?

3.1. Please specify the type and status of service user information that is proposed to share, paying particular attention as to whether the information is of a sensitive nature and consent has been given.

Type and status of information shared:

Is the information 'person identifiable'?	Yes
Has explicit consent been given and recorded?	Yes, except in cases where the patient is unable to give such consent due to a lack of mental capacity as defined under the Mental Capacity Act 2005. In such a case the professional may seek consent from the patient's legal representative if one exists (the patient's Health & Welfare Lasting Power of Attorney) or the clinician will act in the patient's best interests in accordance with the Mental Capacity Act 2005. Good practice requires that this will involve liaison with the family or those close to the patient to ensure a real sense of the interests of the patient are known and considered where possible. Note: the receipt of consent is recorded explicitly on the CMC System.
Is the subject aware that sharing will take place?	Yes
Is the information anonymised?	No

Information items shared:

This list must be comprehensive and include ALL data items that are to be shared.

Data item	**Why shared**
Organisational staff first name, surname, email address, user role	To allow creation of user accounts
CMC Patient record: • Patient demographic details • Patient's consent • Medical Information • Health Overview • Patient and Carer awareness of diagnosis and prognosis • Carer/Next of Kin/Lasting Power of Attorney details • GP and other professional involvements • Community, hospice, and hospital contacts • Social Services (contact details, and details of any relevant social services provided care package) • Case notes • Date and Place of Death More details are available on request.	To give clinicians (e.g. OOH doctors; ambulance crews; GPs; community teams; hospice staff; nursing home staff) and social care workers access to the information 24/7 to promote continuity of care to the patient
CMC Patient Care Plan: • Urgent Care Plan • Disease specific care plans (currently Cardiac, Renal, Motor Neurone Disease, Dementia)***** More details are available on request. * Now incorporated in the main Urgent Care Plan	To give clinicians (e.g. OOH doctors; ambulance crews; GPs; community teams; hospice staff, nursing home staff) and social care workers access to the information 24/7
CMC Reports	To provide information to commissioners and CMC user organisations

Additional comments (including whether this information will be shared with or passed on to any other organisation, third-party or sub-contractors):

No patient identifiable information will be made available for research purposes. (For more details, please see the CMC System Level Security Policy.)

3.2. Allocation of DPA and GDPR responsibilities

3.2.1 For the purposes of the Data Protection Act 2018 ("DPA 2018") all participating organisations shall be joint data controllers of all patient data held on CMC.

3.2.2. Each partner organisation shall be exclusively responsible for ensuring compliance with the data protection principles of the DPA 2018 and the GDPR when uploading data relating to its own patients to CMC and when accessing and subsequently using any patient data held on CMC.

3.2.3. In respect of data relating to its own patients only, each partner organization shall be exclusively responsible for complying with the rights of the data subject as per the GDPR and with obligations arising under the first data protection principle of the DPA 2018 and the GDPR in relation to the provision of fair, lawful and transparent processing of information and in relation to the obtaining of any necessary consents.

3.2.4. In respect of all other personal data processed using CMC partner organisations shall, subject to paragraph 3.2.2 and 3.2.3 above, be joint data controllers with joint responsibility for complying with all obligations arising under the data protection principles of the DPA 2018 and the GDPR.

4. LEGAL BASIS FOR INFORMATION SHARING

4.1. Caldicott Requirements

The Caldicott Principles govern the exchange of patient identifiable information in the health service (NHS bodies) and between NHS bodies and local authority social services departments.

By signing this agreement, all parties concur that all patient identifiable information will be processed and managed in accordance with the following seven Caldicott principles:

- Principle 1. Justify the purpose(s) for using confidential information
- Principle 2. Don't use personal confidential data unless it is absolutely necessary
- Principle 3. Use the minimum necessary personal confidential data
- Principle 4. Access to personal confidential data should be on a strict need-to-know basis
- Principle 5. Everyone with access to personal confidential data should be aware of their responsibilities
- Principle 6. Comply with the law
- Principle 7. The duty to share information can be as important as the duty to protect patient confidentiality

4.2. The Data Protection Act 2018 and the GDPR

The primary legislation and regulations supporting and guiding the appropriate sharing of personal data are the Data Protection Act 2018 and the General Data Protection Regulation which came into effect on May 25 2018.

The Data Protection Act (DPA) 2018 relates to the processing of personal data for living individuals only, and is underpinned by the following six principles from the DPA 2018, sections 34(1) & 85(1), which state that personal data shall be:

- Processed fairly, lawfully and transparently;
- Processed for specified, explicit and legitimate purposes;
- Adequate, relevant and not excessive;
- Accurate and kept up-to-date;
- Not kept for longer than necessary;
- Processed in a secure manner;

The GDPR principles Art 5(1):

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The GDPR adds: “The controller shall be responsible for, and be able to demonstrate compliance with Art 5(1) (‘accountability’).”

In relation to the Coordinate My Care programme, the conditions for processing personal sensitive information are set under the GDPR Article 6.1(a).

Article 6.1(a) of the GDPR

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes

- processing is necessary in order to protect the vital interests of the data subject or of another natural person.

However, there are a number of exemptions within the 2018 DPA Act that allow the disclosure of personal information where there would otherwise be a breach of the DPA 2018 or GDPR, or allow information to be withheld that would otherwise need to be disclosed. For example:

- In connection with criminal justice, taxation or regulatory activities;
- Where disclosure is required by law or is necessary for legal proceedings.

All parties recognise the importance of the Data Protection Act 2018 and the GDPR, and will ensure all personal data that is processed as a result of this agreement is managed in accordance with the legislation and regulation.

Health and Social Care Act, 2012: Duty to share information

Section 251B of the Health and Social Care Act, 2012 ('Duty to share information') provides the legal authority for the sharing of information between health and social care commissioners and providers. The Act requires health and social care commissioners and providers to share information about an individual where it is likely to facilitate the provision to the individual of health services or adult social care in England and is in their best interests. This duty is subject to the right of the individual to object to their information being shared.

4.3. Consent

Consent is defined in GDPR Article 4(11) as:

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Consent of personal data must be freely given, specific, informed and unambiguous. The CMC Patient Information Leaflet should be used as part of the consenting process and what the consenter asked the patient should be recorded, preferably within the CMC care plan Consent section.

The first principles of the Data Protection Act 2018 and the GDPR state that 'personal data shall be processed fairly, lawfully and transparently'. Transparently means being clear and open with individuals about how their information will be used.

If individuals are made aware from the beginning what their information will be used for, they will be able to make an informed decision about whether they want you to process their personal data – particularly when it comes to sharing their information with another organisation.

Unless legal exemptions are applicable, all signatories of this agreement will endeavour to seek informed consent from the individual concerned to share their personal information in cases where disclosure relates to non-care purposes e.g. research and service development.

In seeking consent to disclose personal information for non-care purposes (research and service development), the individual concerned will be made fully aware of the nature of the information that may be necessary to share, who the information will be shared with, the purposes for which the information will be used and any other relevant details including their right to withhold or withdraw consent.

Data subjects have the right to withdraw consent and this mechanism is in place on the CMC care plan to allow this to happen easily and at any time.

All partner organisations are required to inform individuals through publicly available information of the purpose for which information about them may be recorded and shared.

Each organisation's policies and procedures regarding the disclosure of patient data without patient consent must be fully considered and authorised by that organisation's Caldicott Guardian (where one exists) or Information Governance Lead.

4.4. Access to information

Under the Data Protection Act 2018 and the GDPR Article 15, individuals have the right to access personal data held about them. Each partner organisation must have procedures in place for dealing with 'subject access requests' and respond to these within 1 month and must not charge a fee for this.

Information that has been provided by another party may be disclosed to the individual without the need for obtaining the provider's consent to disclose, with the following exceptions when consent must be obtained prior to disclosure:

- The provider has specifically stated that the information supplied must be kept confidential from the service user;
- The information is legally privileged;
- Information will not be shared if it identifies a 3rd party who may have given this information (unless 3rd party consent is obtained).

Should a data controller require information from the Royal Marsden as part of the CMC project, the data controller should forward the subject access request to the Royal Marsden on behalf of the patient whilst processing the request in accordance with their own subject access procedure. Once the data controller has received all the requested information, they should then respond to the subject access request as part of their normal process.

The Royal Marsden will aim to provide all relevant information within 10 working days of receiving the request to avoid any delay.

4.5. Complaints procedure

Each party shall put in place procedures to address complaints relating to the disclosure of information. Parties must also ensure the service users are provided with information about the complaints procedure.

In the event of a complaint relating to the disclosure or the use of an individual's personal information that has been supplied / obtained under this agreement, all parties will provide co-operation and assistance in order to resolve the complaint.

4.6. Please describe how service users will be made aware as to the purpose and content of this Agreement, its impact upon them, their rights and how these may be exercised; include reference to Privacy Notices, Subject Access Requests and Complaints Procedures.

All service users are asked for consent to the processing of their personal data for the Coordinate My Care service, as described in section 3.1 above. In addition, Trust leaflets / posters are displayed to inform Service Users about their rights and how NHS organisations have a duty of confidentiality. For the Royal Marsden – service users' rights to complain and to request copies of medical information are displayed on the website as well as communication materials available throughout the Trust.

4.7. Duty of Confidentiality

Each party recognises the importance of their duty of confidentiality, and will not disclose information to which this duty applies without the consent of the person concerned, unless there are lawful grounds to justify otherwise. In requesting release and disclosure of information from partner organisations, all staff will respect this responsibility.

This agreement also recognises that the duty of confidentiality extends after the data subject has died. If any disclosure is requested, written consent should be sought from the deceased person's personal representative.

Each party will have in place appropriate measures to investigate and deal with inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.

4.8. Breach of Confidentiality

In the event of any personal information being compromised by any unauthorised persons, i.e. accidentally lost or stolen or unauthorised access, the party making the discovery will without delay:

- Inform the information provider (original data controller) of the details of the incident;
- Access their robust breach detection, investigation and internal reporting procedures and take steps to investigate the cause;
- If appropriate, take disciplinary action against the person(s) responsible;
- Take appropriate steps to prevent the incident occurring again;
- Inform the information provider (original data controller) of the details and outcome of the investigation.

Once informed, the information provider will assess the potential implications for the individual whose information has been compromised and if necessary notify the individual, the Information Commissioner within 72 hours, and/or the Police.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

4.9. For organisations undertaking statutory duties please describe:

a) The legal basis that underpins this relationship (e.g. Crime & Disorder Act 1998, Children Act 1989 & 2004, etc.), and/or

b) The requisite duties and powers (express and/or implied) arising from this legal basis that will facilitate the lawful sharing of appropriate service user information. Include reference to any explicit limitations to information sharing and any other statutory and non-statutory regulations and guidance.

Please refer to Appendix A for a list of legislation and guidance. Specifically, the Data Protection Act 2018, the GDPR and the Health & Social Care Act 2012 underpin the information sharing described in this document.

4.10. Termination of Coordinate My Care

Currently there is no expiry date on the Coordinate My Care programme. However, if for any reason the project is discontinued, or should a particular locality decide to discontinue use of CMC, each data controller must ensure they collect all the relevant information they require for their own patients. The Royal Marsden as host will hold the information until it has been retrieved accordingly.

Should any information not be retrieved, then the Royal Marsden will store and archive the patient data in line with its own facilities and retention schedule. Information will of course be made available to signatories of this agreement during the retention period.

5. SERVICE USER CONSIDERATIONS

5.1. Privacy and confidentiality

Please describe what steps will be taken to minimise the impact on service user's privacy and/ or confidentiality – noting whether a 'Data Protection Impact Assessment' has been conducted.

A data protection impact assessment has been carried out on CMC and is distributed to CMC user organisations alongside the current document.

5.2. Information Security

Each party will:

- Ensure that all personal information that has been disclosed to them will be recorded accurately on that individual's manual or electronic record in accordance with their policies and procedures
- Parties will continue to comply with all obligations and requirements in relation to information security, for example an appropriate NHS Digital Data Security and Protection Toolkit, and will make all the relevant assertions as required by the toolkit.
- Only transfer, store, and manage personal data as specified in this agreement
- Ensure only those with authorised access rights to the CMC System can access it
- Conduct regular auditing of user access to the CMC System and monitor compliance
- Ensure that employees who need to share personal information under this agreement are given appropriate training and made fully aware of their responsibilities to maintain the security and confidentiality of personal information
- Staff who are not directly involved with sharing personal information should not be excluded from such training as it is possible they may come across such information during the course of their duties.
- By signing this document all organisations agree to accept this ISA and to adopt the statements and procedures contained within it and any associated documents.

5.3. Please describe who will have a right of access to the information provided as a result of this ISA, how it will be managed and what procedures are in place to prevent unauthorised access/disclosure; include reference as to whether access will be varied/restricted in accordance with roles or the sensitivity of the services provided and whether appropriate Disclosure and Barring Service (DBS) clearance is required.

All signatories of this agreement have access to this information. However, access will be managed as joint responsibility between the organisations. The Royal Marsden will remind organisations on a bi-monthly basis to keep access accounts up to date, and organisations will ensure this is the case. Each health or social care professional is obliged to declare a Legitimate Relationship (which is recorded on the CMC System), indicating that they are working directly with the relevant patient, before they can obtain access to any CMC care plan. The publishing (approval) of a new CMC care plan by a health or social care professional implicitly declares such a Legitimate Relationship; in all other cases the declaration is explicit. All staff will receive CMC training or access to training resources, which covers CMC-related Information Governance requirements, and will also read and sign/electronically confirm agreement to the Acceptable Use Policy. Staff are also required to complete IG training as mandated under the NHS Digital Data Security and Protection Toolkit that covers their organisation.

5.4. Please note that *data is not transferred between the parties to this agreement*, being stored as a single instance and accessed by all users via the same browser-based CMC application, except as follows:

Name of data flow	Data included	Frequency	Purpose of transfer	Nature of transfer
CMC GP practice email notifications (following any change to a CMC record for a patient of that practice)	Forename Surname Date of Birth Gender NHS Number Every data item that has been edited, showing values before and after change	Potentially every 4 hours	Notify relevant GP practice of existence of new or amended CMC records	nhs.net email between Intersystems and relevant organisation
CMC Urgent Care Service email notifications	Forename Surname Date of Birth Gender NHS Number Address	Potentially every 4 hours	Notify relevant Urgent Care Services of existence of new or amended CMC records (driving addition or removal of CMC existence flags on urgent care service systems)	nhs.net email between Intersystems and relevant organisation
CMC Urgent Care Service automated flagging	NHS Number Title Forename Surname Gender Date of Birth Date of Death Address(es) and postcode(s) Telephone number(s) Email address(es) Patient Category (End of Life Adult)	On demand, typically every 4 hours	Notify relevant Urgent Care Service of new or amended CMC records (driving addition or removal of CMC existence flags on urgent care service systems)	Use of CMC Automated Flagging web service
Reconciliation extracts for Urgent Care services	Typically: Forename Surname Date of Birth Date of Death NHS Number Address and Postcode Phone number Gender	Occasional	Reconciliation extracts for Urgent Care services (used to check existence flags)	nhs.net email between RMH and relevant organisation
Demographics Changes Reports for Urgent Care services (obsolete)	Surname Gender Date of Birth Date of Death Address and Postcode Forename Plus old and new versions of modified demographics item	Daily when there are relevant changes	Maintenance of accurate existence flags	nhs.net email between RMH and relevant organisation
Audit reports for CMC user organisations	Surname, gender, date of birth only	Typically monthly	CMC Team Audit Reports for CMC user organisations (used in these organisations' service quality assessment)	nhs.net email between RMH and relevant organisation

Name of data flow	Data included	Frequency	Purpose of transfer	Nature of transfer
Data Quality reports for CMC user organisations	Surname, gender, date of birth to identify patient. Other data as just sufficient to describe the data quality issue encountered on that patient's CMC record	As required, probably not more than weekly	Data Quality (exception) reports for CMC user organisations	nhs.net email between RMH and relevant organisation
Migration of care coordination data relating to organisation moving to use of CMC	Any CMC data item	As required (very occasional)	Migration of care coordination data relating to organisation moving to use of CMC	Email to RMH via nhs.net, then SFTP to Intersystems over VPN tunnel
Migration of CMC data to new platform, 24.11.2015 (obsolete)	Potentially all CMC data items	Once	Migration of potentially all CMC data except that relating to patients marked deceased on the Spine as of 23.11.2015	Transfer via VPN tunnel from System C data centre to RMH, and then via VPN tunnel from RMH to Intersystems
Entry of hospice CMC information by CMC team or other CMC user organisation	Potentially all CMC data for patient, as above	On demand	Entry of hospice CMC information (only for hospices with no N3 connection)	Hardcopy CMC form faxed by hospice
Spine reconciliation of CMC data	Sent: NHS Number Forename Surname Date of Birth Gender Postcode Received: NHS Number Date of Birth Fact of Death Date of Death Surname Forename Gender Address and Postcode	On demand, typically approx. monthly	Spine reconciliation of CMC data	DBS (PDS batch) trace processed by RMH Information Department
CMC operational reports, e.g. Patient List Report	Depends on report - details available on request.	On demand	Patient care coordination, e.g. palliative care meeting	Access to CMC application hosted at Intersystems. Data may be printed or otherwise stored locally for use in a meeting.

Name of data flow	Data included	Frequency	Purpose of transfer	Nature of transfer
CMC automated flagging for Camden Integrated Digital Record	NHS Number Title Forename Surname Gender Date of Birth Date of Death Address(es) and postcode(s) Telephone number(s) Email address(es) Patient Category (End of Life Adult)	On demand	Notify Camden Integrated Digital Record service (Camden CCG) of new or amended CMC records (driving addition or removal of CMC existence flags on urgent care service systems)	Use of CMC Automated Flagging web service
CMC Availability Service and In-Context Link capability (data flow incoming to CMC only)	NHS Number Date of Birth	On demand	Availability Service allows partner system (e.g. EMIS Web) to identify whether or not a CMC care plan is in place for the relevant patient In-Context Link invokes normal CMC Search function for specified NHS Number/Date of Birth Note that all Availability Service calls, whether made from a current CMC user's local system session or not, are logged securely (organisation identifier, NHS number, Date of Birth) by CMC's Managed Service provider for incident investigation purposes.	Use of CMC Availability Service web service Use of partner system In-Context Link API (e.g. EMIS Portal SDK) to invoke CMC functionality
CMC CLI (Telephone Number) Extract for 111 service in London	Patient telephone number (home, mobile, work, etc.) GP practice ODS code CCG ODS code 111 provider	Daily	Used by Redwood (111 London telephony and contact centre automation provider) to ensure, as far as possible, that calls from CMC patients are routed to their local 111 provider	nhs.net email between RMH and Redwood

Name of data flow	Data included	Frequency	Purpose of transfer	Nature of transfer
CMC Crisis Care Extract (CCE) service for 111 service in London	Professional Record Standards Body (PRSB) CCE standard. Details available from CMC on application.	On demand (Yet to be deployed)	Real-time request from 111, for a specified NHS number, to retrieve either CMC information for that patient, transformed to CCE format, or an indication of its absence. The 111 clinician will be shown the information via Adastra's Special Patient Note (SPN) functionality.	IHE standard interoperability calls from Redwood to new on-demand CMC service, exposing CMC data transformed to meet the PRSB CCE standard and delivered as a CDA Level 3 document. The retrieved data will then flow from Redwood to form an SPN in the relevant Adastra instance.

5.5. The retention and destruction of personal information must be managed in accordance with each party's retention schedule and confidential disposal procedure.

Please describe how service user information will be recorded and held; include reference as to the Accuracy, Security, Retention, Destruction and Future Use of the information. Take into account any current recording and holding methods i.e. encrypted device, network.

Service user information is stored within the CMC database. Information will be 'soft deleted' if no longer required, e.g. if patient consent is withdrawn. Soft deletion involves removing the care plan from view from the CMC platform - a search for the care plan will not return a plan. Complete removal of a CMC record from the database is also possible should specific circumstances mandate this. Data relating to deceased patients is retained for 30 years (RMH standard retention period) and will then be removed completely from the database.

Information Sharing Agreement

SUMMARY OF ENDORSEMENTS – SIGNATURE/CONFIRMATION SHEET

Coordinate My Care

The parties to the agreement are as follows:

Organisation: **NHS Org. Code:** **Address:**	The Royal Marsden NHS Foundation Trust RPY 203 Fulham Road, London SW3 6JJ
Signature:	
Name:	Dr Nicholas van As
Designation:	Medical Director & Caldicott Guardian
Date:	17/10/2018

Organisation or Organisations covered by this signature, with addresses, and showing NHS Org. Code(s) where relevant: (please print)	
Signature or, if submitting electronically, 'Please accept this as formal confirmation':	
Name: (please print)	
Telephone:	
Email: (please print)	
Designation:	Caldicott Guardian
Date:	

An up to date list of participating organisations may be obtained from the Coordinate My Care Team upon request.

Appendix A: *Legislation*

The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates this. Below is a non-exhaustive list that is of relevance:

- The Data Protection Act 2018
- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Human Rights Act 1998
- The Mental Health Act 1983
- The Children Act 1989 (sections 17, 27, 47 and Schedule 2)
- The Children Act 2004 (sections 10, 11 and 12)
- The NHS & Community Care Act 1990
- The Access to Health Records Act 1990
- The Carers (Recognition & Service) Act 1995
- The Crime & Disorder Act 1998
- The Health Act 1999 (section 31)
- The NHS Act 2006 (section 251)
- The Local Government Act 2000 (section 2)
- The Local Government Act 1972 (section 111)
- The Education Act 1996 (sections 10 and 13),
- The Education Act 2002 (section 175)
- The Learning and Skills Act 2000 (sections 114 and 115)
- The Crime and Disorder Act 1998 (section 115)
- The NHS Confidentiality Code of Practice
- The NHS Records Management Code of Practice
- The Access to Health Records Act 1990
- The Mental Capacity Act 2005
- The Health and Social Care Act 2012

It is essential that care professionals sharing information are clearly aware of the legal framework within which they are operating. The latest GMC guidance on patient confidentiality, which can be found at http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp, is a useful source of information. All organisations will also meet the commitments outlined in the NHS Care Record Guarantee.

Department of Health Confidentiality Code of Conduct 2003; http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253