The Royal Marsden NHS
NHS Foundation Trust

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

Purpose Specific Information Sharing Agreement (PSISA)

This Purpose Specific Information Sharing Agreement (PSISA) is to identify:

- The organisations/parties/individuals involved in the collection and sharing of information
- The procedures for securing and confidential sharing of information between the organisations/parties
- The method of collection of personal information by the organisation/party
- How this PSISA will be implemented, monitored and reviewed.

Service / Team / Project Name:	Coordinate My Care
Date of completion:	14/04/2021
Completed by:	Marta Mulyak CMC Clinical Quality Manager and Alan Ball Royal Marsden Hospital IG Lead
Review Date:	Annually

Information sharing agreement

This proforma should be completed for each information sharing agreement set up between two or more partner organisations. It should be completed by the individuals who will be managing the sharing of information on a day to day basis (i.e. practitioners), signed and agreed by the Service Director or functional equivalent and Caldicott Guardian/Designated Officer.

Introduction:
The parties to the agreement recognise that organisations need to work closely together in order to provide integrated services to patients and service users. 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.

The purpose of this agreement is to formalise the data sharing arrangement between the specified organisations, whilst outlining the agreement's compliance against Information Governance standards.

Each organisation that supplies patient information to the CMC platform is the Data Controller of that information and has specific responsibilities toward it. 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. By signing this agreement, each partner organization agrees that all other partner organisations may access, amend and manage information relating to its patients as is appropriate and justifiable, in line with the terms of this agreement.

No.		Response/ Details
1. What is being shared?		
1.1	What sort of information do you intend to share	☒ Identifiable ☐ Pseudonymised ☐ De-identified ☐ Aggregate
1.2	Describe the purpose for sharing information?	Coordinate My Care (CMC) is an NHS initiative, run by The Royal Marsden NHS Foundation Trust and operational since August 2010, permitting the provision of clinical 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 with a legitimate relationship, and by patients and carers. Non-urgent care providers collaborate to establish, maintain, and use the Urgent Care Plans of their

No.		Response/ Details
		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 future care needs and plans of patients who have been identified with complex ongoing health needs (which may include patients at the end of life, or with Heart Failure, Chronic Pulmonary Airways disease, Dementia or Frailty). • 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. A CMC Patient Care Plan is created and made available to view and/or update to the following services with a legitimate relationship: • clinicians (e.g. OOH doctors; ambulance crews; GPs; hospital teams, community teams; hospice staff; care home staff) • social care professionals • support staff including administrators working on behalf of health and social care professionals • other care and support providers working in collaboration with and/or on behalf of health and social care to deliver care and support to patients.
1.3	Describe the information you intend to share? What data fields/type of information	**Information regarding the staff who are to receive CMC access:** Staff first name, surname, email address, job role. This is to allow creation of user accounts. **Information regarding the patient and the patient:** CMC Patient record:

No.		Response/ Details
		• 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 contact 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.
2. Benefits test:		
2.1	What outcomes are you seeking to achieve through sharing information?	To promote improved outcomes for the patient • To ensure the patient wishes are known. • To increase opportunities for care and treatment to align with patient wishes and values where possible. • To increase opportunities for the patient to receive the right care in the right place by the right team through the availability of the right information. • To support services to ensure the patient is cared for on the best care pathway for them which may include reducing inappropriate and avoidable hospital admissions • To reduce the need for requests to the patient for basic and previously provided information and reduce the burden on the patient at stressful times to repeat basic and important information.

No.		Response/ Details
2.2	What benefit do you expect to be accrued to your organisation, the partner(s) providing the information and the people who the information may be about?	Increased quality of care and harm reduction to the patient. Increased alignment of care and treatment with patient wishes and values. Increased efficiency of service utilisation – services being deployed according to commissioned purpose (for example utilisation of the rapid response team to support the patient and avoid inappropriate admissions for the patient). Increase availability of services for other work demands (for example ambulance crews being more available to convey patients to hospital as they may be released from an incorrect care response where conveyance is not advised.

3. Basis for sharing?		
3.1	Legal basis for sharing the personal information Article 6 of the General Data Protection Regulation 2016/679	For the creation of a CMC care plan Article 6(1)(a) is the legal basis (consent, as defined in data protection legislation). • An indication of consent provision by the person who has mental capacity to agree to having the support of a CMC care plan is required on the CMC care plan. (Where mental capacity to agree to having a plan is not available, the consent of the Lasting Power of Attorney for Health and Welfare where one exists or where not, the clinician's decision in the best interests of the patient may be used. • Any process by which consent is obtained, how the discussion and decision are undertaken, gained and otherwise noted is the responsibility of the individual controller organisations to design and manage. For viewing (processing) the record by services including urgent care services Article 6(1)(e) is the legal basis (performance of a public task).
3.2	Legal basis for sharing the information ***special categories*** of personal information i.e. health information	For the creation of a CMC care plan Article 9(2)(a) is the legal basis (consent, as defined in data protection legislation).

	Article 9 of the General Data Protection Regulation 2016/679	• An indication of consent provision by the person who has mental capacity to agree to having the support of a CMC care plan is required on the CMC care plan. (Where mental capacity to agree to having a plan is not available, the consent of the Lasting Power of Attorney for Health and Welfare where one exists or where not, the clinician's decision in the best interests of the patient may be used. • Any process by which consent is obtained, how the discussion and decision are undertaken, gained and otherwise noted is the responsibility of the individual controller organisations to design and manage For viewing (processing) the record by services including urgent care services Article 9(2)(h) is the legal basis (medical purposes).
3.3	Legal Basis for sharing under the Common Law Duty of Confidence (see appendix)	Implied consent. Health and Social Care Act requires health care providers to share information to enable direct care to take place.
3.4	If aggregated data for secondary uses, not direct care, consider whether any individuals may be identifiable from the information (and in conjunction with any other information available) If personal data, consider whether the information can be provided in an anonymised way.	Data may be used for auditing and service evaluation purposes whereby information is accessed by legitimate organisations and services which the patient had previously utilised or is utilising currently. The end product of any audit (report or similar) and service evaluation (report or similar) will not contain patient identifiable data. Controller organisations wanting to access historical information that no longer is available on their view of the care plan due to update changes made on the care plan over time, can be provided with that information by the Coordinate My Care service on request. The controller identifies the persons of interest to them and will communicate this to the Coordinate My Care service so that they can retrieve and transfer the relevant items to the requesting Controller organisation via a secure email transfer.

3.5	Data Privacy Impact Assessment – please embed DPIA in box opposite for high risk processing. Does a residual risk remain? Describe DPIA's are require to be published	 CMC DPIS.pdf No. Published on the CMC website. https://www.coordinatemycare.co.uk/joining-cmc/

4. People who the information is about (if personal data)		
4.1	Describe affected data subjects (people who the information is about).	Persons who wish to benefit from key information including their views, wishes, clinical perspective on future management being available across the health and social care system to inform responses to their needs as they arise in the future. This will include those who are at the end of life or those with heart failure, Chronic Obstructive Pulmonary Disease, frailty or dementia or similarly complex conditions, or those who are in a stable health state but considering their future.
4.2	If personal data, describe the arrangements for obtaining consent (if this is the legal basis for the sharing) or informing data subjects affected what information will be shared and why (Privacy Notice statement in accordance with GDPR / Data Protection Act), or state exemptions to this.	For clarity, there is no such item as a non-available/non-shared CMC care plan. The patient's explicit consent is required for the patient to have a plan in the first instance, the purpose of which is to be available to other appropriate persons where required. The nature of the CMC care plan (how it works) is to be made known to the patient when consenting to have the support of a CMC care plan. Therefore separate consent is not required for each instance of sharing or subsequent processing (including viewing or updating) of the plan that has been consented to. Standard practice for gaining consent – provision of information, opportunity for clarifying questions, time to consider, information about withdrawing consent are assumed as part of everyday clinical and professional practice with patients and is similarly applicable and therefore required when gaining consent to have a CMC care plan.

5. Controls		
5.1	How will the information be transferred (e.g. paper, email, secure email, access to web portal, machine to machine etc.)	Transferred through an integrated digital system provided by Intersystems. See section 5.3.
5.2	How and where will the information be held? (e.g. will the data be shared with any subcontractor?	United Kingdom. See section 5.3 for information about the CMC system provider.
5.3	What **security** arrangements do you or will you have in place (technical and organisational)? Include: • Technical • Systems • Office security • People management • Training • Security when transferring information • Confidential waste etc. *Security arrangements should be commensurate with the type of information shared and the risk.	The CMC solution is provided as a hosted, managed service. The data is held securely in 2 United Kingdom based data centres by our hosting and managed service partner InterSystems. InterSystems, who provide the CMC IT solution as a hosted managed service, is responsible for the confidentiality and security measures used to store CMC IT solution data, including myCMC, the CMC patient Portal. These robust measures are defined by the Coordinate My Care Service Agreement between InterSystems and The Royal Marsden NHS Foundation Trust. These include but are not limited to: □ Quality management and certification, e.g. ISO9001. □ ISO/IEC 27001: 2005: Information Security Management Systems: Requirements. □ ISO/IEC 27002: 2005: Code of Practice for Information Security Management. □ NHS Digital Data Security and Protection Toolkit compliance. □ Trust's IT Acceptable Use Policy and IT Security Policy conformance. □ System Security Plan (SSP) provision, including a Data Protection approach production. □ Best practice operational security plan for CMC system live operation production.

		The CMC governance model encompasses this 1) Data Sharing Agreement and compliance with 2) Data Security & Protection Toolkit - Standards Met level, 3) individual login credentials providing access to the care plan (from the CMC service or through a federated model where relevant information regarding the organisational user approaching the CMC system is provided through an in-context approach to the CMC relevant care plan), 4) individual acceptable use policy commitment, 5) legitimate relationship claim on accessing the care plan, and 6)full audit trail. All potential users to CMC will be validated through provision of an nhs.net/nhs.uk email account by the applying individual or through being listed on a User Access Form which is produced by a team/organisational senior. Controller organisations take responsibility for staff training in and adherence to appropriate governance standards. All users of the CMC solution will have completed annual data protection and cyber security training. Training resources on how to use the CMC platform effectively and safely are available to from the CMC service for all user types. Organisations of reasonable size may take upon themselves the responsibility of integrating and delivering CMC training to staff as they join their organisation and the Corporate Training Model Policy document will be used to support this approach and place responsibility with the controller organisation that choose this approach.
5.4	What arrangements (if needed) are in place to arrange for **updates** of the information to be shared? This should also include corrections or deletions or amendments to personal data, under the Data Protection Act.	The CMC system has an update function which CMC users can access to update the care plan to reflect the latest expression of patient preferences, the latest clinical status and recommendations for future clinical management. The CMC care plan template has a link to the Personal Demographic Service (PDS) to allow updating of demographics and current GP details. A CMC user can access this link to update demographics, GP practice details and date of death. Care plan subjects (patients) can be enrolled to view their own CMC care plan and request changes through the CMC patient portal myCMC.

		Where the patient informs their clinician that they wish to withdraw consent to having a CMC care plan, it can be withdrawn from view by the clinician directly. The CMC care plan system contains a work flow management cycle reminding users through internal (on screen Action Needed list) and external means (email prompt to deliver task completion) to finalise draft care plans, review care plans when their review date becomes due.
5.5	If applicable, how will **accuracy** of the information be maintained?	Responsibility for care plan maintenance with regard to accuracy of information and correspondence to the patient's situation is held by the relevant clinicians utilising CMC to support their patient. The CMC care plan has a link to PDS as above. Additionally, CMC service carries out regular reconciliation reports against the PDS to ascertain inaccuracies as to primary demographic items – forename, surname, gender, date of birth, address. Inaccuracies can occur when the CMC user bypasses the demographics load from PDS and incorrectly enters details manually. CMC can then update the care plan directly or liaise with the CMC user most appropriate to carry out this function if appropriate in order to achieve accuracy.
5.6	When and how (technical description) the information will be **disposed** of? *Where personal data, information should not be kept for longer than necessary and be disposed of securely.	InterSystems, which provide the CMC IT solution as a hosted managed service, is responsible for implementing the record retention and destruction policy. Schedule 12 of the Coordinate My Care Service Agreement between InterSystems and The Royal Marsden NHS Foundation Trust defines the Exit Plan and Termination Services, including "(1.14.10) the migration of all relevant data and information stored and/or processed by the CMC Solution to the Trust or any Incoming Supplier, and/or at the request of the Trust the return of any data or information relating to the CMC Solution or certification by the Supplier of its permanent deletion". InterSystems' data deletion process is fully compliant with the NHS Destruction and Disposal of Sensitive Data: Good Practice Guidelines (v3.2 January 2017) ("NHS Guidance") in that those steps involved in our procedure fully follow the requirements of the Purge Level under NIST SP 800-88, Guideline

		for Media Sanitization (Rev. 1 December 2014) ("NIST Guidelines"). "Where individual records are modified and/or deleted in the database e.g. as part of normal operations the storage for that record is not securely deleted but simply made available for use within the same database. We do not believe this to be a requirement and doing so would not be practical for most databases. Similarly, backup schedules will render backups unrecoverable after 12 months but this is not a secure overwrite but rather a discard. Data blocks will likely be overwritten quickly." (From Intersystems) Where myCMC Initiate requests for care plans are not updated and submitted to the CMC system, they are retained for 60 days, after which time they are automatically deleted. Individuals can create another request at any time. Once a myCMC Initiate request for a care plan has been submitted to the CMC system and the care plan has been finalised and clinically approved it becomes subject to the NHS Records Management Code of Practice for Health and Social Care 2016 (retention schedules) as per all other CMC care plans.
5.7	What is the **retention** period of the personal data being shared?	See 5.6 above.
5.8	Are audit trails available of who has accessed/added/edited/destroyed any personal data?	Yes, CMC has a full audit trail.

6. Assurances – information providing organisation to complete		
6.1	Describe any details about the accuracy of the information and how accuracy is assured.	The relevant data controllers (clinicians working with the data subjects - patients) will take all reasonable care to enter accurate information onto the CMC care plan. The relevant data controllers will maintain the accuracy of the CMC care plan through timely updating of the care plan as appropriate, no less than a yearly review and update of the care plan time stamp. The CMC service runs reports monthly to identify any accuracy issues and will address them within a

		timely manner directly or through collaboration with the relevant (data controller) clinical team.
6.2	What (if any) restrictions are to be placed on the specific use of this information?	Information is to be used for the purpose of direct care provision to patients. Information may be used for the purpose of audit and service improvement where no identifiable data appears in the output produced – report or similar. Any transfer of identifiable data between CMC and the auditing organisation, where a legitimate relationship is in place, so as to enable the audit questions to be addressed, is transferred from an nhs.net to nhs.net email account and to an appropriate identified person within the auditing organisation. Controller organisations who wish to access data on CMC for the purpose of service improvement utilising clinical audit methodology will only access relevant data for patients they have or have had a legitimate relationship to. Where CMC needs to provide information to support such an exercise, information will only be provided where they are satisfied that the information is relevant to the organisation. As the care plan is multidisciplinary and multi service in nature, an inter-service clinical audit may be carried out to support service improvement and CMC where required will provide information via a secure email and where they are satisfied that the parameters of the request and parties are relevant to the information being requested. Access control is operational within the CMC system. The intended user's 'organisational role' will be provided to the CMC service, so that the correct restrictions may be activated against the individual users details during set up on the CMC system e.g. a practice manager's user type on CMC will enable them to enter data on behalf of their clinical colleague but disable the clinical approval function and offer the 'submit for approval' function. Username and password are provided to persons who have been listed by their senior in a form requesting access (User Access Form) and where the information sharing agreement has been signed. Alternatively, individuals may request access credentials to CMC directly, where nhs.net and nhs.uk email account types will be used to validate

		the recipient. The request will then be processed by the CMC team.

7. When and how frequently will sharing take place?	
Frequency of information transfer?	Information is not transferred, information is accessed when the service user interacts with the Urgent Care Services or when a clinician with a legitimate relationship to the patient needs to access the information for the purpose of increasing their understanding, or are updating or reviewing the care plan. This may be weekly or yearly depending the needs of the patient.
Start date	2010. This ISA is an updated version to reflect current Data Protection legislation.
End date	On-going. Would end if the CMC service was terminated.

8. Arrangements for review		
8.1	Is a review of this arrangement required?	Only when legislative changes would require a review or if an incident review recommended a review.
8.2	If yes, state date for review / or specify time frame for regular review.	See above

Section 9: This Information Sharing Agreement must be signed and agreed by the Service Director or functional equivalent and Caldicott Guardian/Designated Officer for each organisation.
Information Sharing Agreement **SUMMARY OF ENDORSEMENTS** **Coordinate My Care**

The parties to the agreement are as follows;

Organisation **Address** **Contact Details**	The Royal Marsden NHS Foundation Trust [ICO Reg: Z5146911] 203 Fulham Road, London SW3 6JJ
Signature	
Name:	Eamonn Sullivan
Designation:	Chief Nurse & Caldicott Guardian
Date:	28.02.2020

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

An up to date list of all participating organisations to this Joint Controller Agreement may be obtained from the Coordinate My Care Team upon request. As of February 2020, there are 1400 participating organisations - controller organisations - party to this agreement. This will include Hospital and Community NHS Trusts, GP practices, hospices and care homes.

General Data Protection Regulations (GDPR) / Data Protection Act - Conditions for processing personal and sensitive personal data

ARTCILE 6 - Conditions relevant for processing of any personal data

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

ARTICLE 9- Conditions relevant for processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact

with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; 4.5.2016 L 119/38 Official Journal of the European Union EN

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

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
- 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 Health and Social Care Act 2001 (Section 60)
- 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 Civil Contingencies Act (2004) Part 1 and supporting regulations
- The Access to Health Records Act 1990
- The Mental Capacity Act 2005

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

[End of Document - Do Not Delete]