

Data Protection Impact Assessment Form

Please complete all the fields below to the best of your knowledge and send to the Information Governance Manager for review.

Department:	Coordinate My Care (CMC)	
Department Lead	Name	Julia Riley
	Title	Clinical Lead
	Telephone	0207 811 8490
	Email	Riley, Julia <Julia.Riley@rmh.nhs.uk>
Information Asset Owner (if different to above)	<i>As above.</i>	
Date of when processing is due to commence:	24 th November 2015	

Key Information	
Name of project / processing	Coordinate My Care Service – utilised to support future care planning with and for consenting persons.
Description of project/processing: <i>Please provide a clear summary description of what your project will do and deliver.</i>	<p>Coordinate My Care digital urgent care plan can be used to support consent based care planning in preparation for future crisis or deterioration and engagement with urgent care services. The care plan is a combination of patient wishes and preferences, and clinical recommendations so that future responses by clinical and care teams including Urgent Care Services can be aligned to the person’s wishes and clinical recommendations.</p> <p>CMC care plans are created by clinicians working with patients or where mental capacity is absent with regard to agreeing to the support of a CMC care plan, working with an appropriate Lasting Power of Attorney if present, or in the patient’s best interests. Care plans may be initiated by the person themselves, hereafter referred to as the patient, through the CMC patient portal, myCMC.</p> <p>myCMC is an integral part of the CMC IT solution. Patients can: initiate their urgent care plan; view their clinically approved plan (whether they initiated it or not), which is available to urgent care; and request changes to their clinically approved plan. myCMC patient initiated plans and requested changes are processed by clinicians in the CMC system. Authorised patient ‘Proxies’ can also view the patient’s care plan via</p>

	<p>myCMC.</p> <p>Benefits of CMC include: CMC urgent care plans are available to all patients in the area that the CMC service is commissioned; the service is particularly relevant for patients with complex needs, for example those suffering from long term conditions; the frail and elderly; and patients who are at the end of life.</p> <p>Benefits include more personalised care responses, and patients being cared for in their preferred place.</p> <p>The right information is available to the right people in the right place and at the right time. Patient wishes, preferences and clinical information are shared across care settings, including urgent & emergency care. This information is known, understood and respected.</p> <p>Unnecessary and unwanted hospital admissions and associated costs to care services are reduced. Associated patient and family distress are reduced.</p> <p>Where 'myCMC Initiate' is used: Patients are more prepared for meeting their doctor or nurse and for potentially difficult conversations and decisions; Care plans are created more quickly and easily by the clinician; Care plans are of better data quality due to the data already recorded and submitted by patients; Patients are better informed and involved in their plan and associated care;</p> <p>Advance or future care planning allows the patient and the clinical team through discussion prior to care plan creation on CMC to deepen understanding and bring some alignment regarding future management and treatment responses.</p>
--	---

Type of Personal data to be processed

Personal Data	Please tick all that apply	Sensitive Personal Data	Please tick all that apply
Name	✓	Racial / ethnic origin	✓
Address (home or business)	✓	Political opinions	
Postcode	✓	Religious beliefs	✓
NHS No	✓	Trade union membership	
Email address	✓	Health: Physical or Mental	✓
Date of birth	✓	Sexual life	
Payroll number		Criminal offences	
Driving Licence [shows date of birth and first part of surname]		Biometrics; DNA profile, fingerprints	
		Bank, financial or credit card details	
		Mother's maiden name	
		National Insurance number	
		Tax, benefit or pension Records	

	Adoption, employment, school, Social Services, housing records	
	Child Protection	
	Safeguarding Adults	
Additional data types (if relevant)	<p>The following CMC urgent care plan data items are processed within the CMC urgent care plan Consent category</p> <ul style="list-style-type: none"> Title Name Preferred Name Aliases Addresses Accommodation & Access information Patient contact details Date of Birth Gender Marital Status Religion Ethnicity Preferred Language NHS Number Registered GP Practice Registered GP Alerts Diagnoses Patient & Family awareness of diagnosis Prognosis Patient & Family awareness of prognosis Advance Decision to Refuse Treatment Other significant history Disabilities WHO performance Status Place of Care & Place of Death Preferences Organ Donation Thoughts Patient Wishes Family awareness Cultural & Religious Needs Cardiopulmonary Resuscitation Patient Discussion 	
	<ul style="list-style-type: none"> Cardiopulmonary Resuscitation Family Discussion Cardiopulmonary Resuscitation Decision Ceiling of Treatment/Clinical recommendations Emergency Treatment Plan Allergies Medication Health & Social Care Contacts & Contact Details Personal Contacts & Contact Details Health & Welfare Lasting Power of Attorneys & Contact Details Care Funding, Help & Support Urgent care event history and event note myCMC- patient and proxy enrolment status Document attachments e.g. discharge letter 	

Lawfulness of the processing – personal/ sensitive personal data

Please indicate which <u>one</u> of the following legal conditions you are relying on for processing	
Condition	Please tick all that apply
Explicit consent	
Is the processing for a medical purpose – e.g.;	✓
• Articles 6(1)(e) (public task) and 9(2)(h) (medical purposes)	
Processing is required to protect the vital interests of the person – e.g.;	
• Articles 6(1)(d) (vital interests) and 9(2)(c) (vital interests)	
Further Processing:	
Is any processing going to be by a not for profit organisation, e.g. a Charity	✓
Would any processing use data already in the public domain?	
Could the data being processed be required for the defence of a legal claim?	✓
Would the data be made available publically, subject to ensuring no-one can be identified from the data?	
Would the data be made available publically, for public health reasons?	
Will any of the data being processed be made available for research purposes? (recital 33 of GDPR)	✓

Legal basis for creating a CMC Plan	Article 6 (1) (a) – the data subject has given consent to the processing of his or her personal data for one or more specific purposes; Article 9 (2) (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.
Legal basis for accessing CMC plan	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 vested in the controller. Article 9 (2) (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.

<u>Description of data processing</u>	
Answer all the questions below for the processing of Personal Sensitive Data	
How do you intend to make people aware of this processing?	<i>e.g. update privacy notice, write to them, use of posters.</i> CMC website: https://www.coordinatemycare.co.uk/ , CMC Terms of Use: https://www.mycmc.online/public/index.html#/info/termsDisplay ,

	<p>CMC Privacy Policy: https://www.coordinatemycare.co.uk/privacy-policy/,</p> <p>CMC Patient Information Leaflet: https://coordinatemycare.co.uk/wp-content/uploads/2018/12/cmc-patient-leaflet-september-2015.pdf,</p> <p>myCMC Step by Step Guide: https://www.coordinatemycare.co.uk/wp-content/uploads/2019/05/cmc_step-by-step-patient-guide.pdf</p>
Will the data be linked with any other data collections?	No.
Will any of this information be new information as opposed to using solely existing information in different ways?	No. It involves making existing information available in a different way.
Who will be able to access identifiable data?	<p>The following will have access to the identifiable data:</p> <ul style="list-style-type: none"> • The patient through myCMC, the CMC patient portal. • The patient's nominated proxies through myCMC. • All health & social care providers who are CMC service users via the CMC clinical system.
Are there any plans to allow the information to be used elsewhere within the organisation, wider NHS or by a third party?	<p>The purpose of the CMC service, including the CMC patient portal – myCMC, is to enable the sharing of patients' urgent care plan information with the wider health and social care providers who are CMC service users, and with the patient and their proxies themselves.</p> <p>There are no current plans to allow the information to be used more widely than the care settings and organisations outlined in the project description.</p>
What is the justification for the inclusion of identifiable data rather than using de-identified/ anonymised data?	Direct care. Identifiable data is necessary to enable health and social care providers to access patient specific urgent care plan information when caring for individual patients.
Do you have procedure in place to give the data subjects the possibility to correct their personal data or to ask for a correction of their personal data (rectification)?	<p>Yes. When creating a CMC urgent care plan request using 'myCMC Initiate' the patient / data subject is effectively the data controller who controls the accuracy of the data they are providing. At any time up to submitting their myCMC Initiate request for a care plan to a doctor or nurse, the patient can amend any of the information they have already provided, or cancel their request entirely, and the information that they had provided is deleted.</p> <p>Once the patient's request for a CMC urgent care plan is submitted and the patient attends an appointment with a doctor or nurse to confirm their identity and consent to a care plan, medical information is added and the plan clinically is approved, the patient / data subject can be enrolled to view the care plan and may request changes to their plan through myCMC.</p>

<p>How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?</p>	<p>If 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.</p> <p>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).</p>
<p>Are procedures in place to provide access to records under the subject access provisions of the DPA (and GDPR)?</p> <p>Is there functionality to respect objections/withdrawals of consent?</p>	<p>Yes.</p> <p>The data controller organisation whose staff will place information onto the CMC care plan platform will contact the CMC service (the data processor on their behalf), to support their response to the Subject Access Request (SAR). The Controller will be able to access the relevant information and provide it to the person as a PDF or printed copy. The CMC service will highlight on request the existence of any other controller organisations that have been involved in creating/maintaining the care plan and provide their details to the Controller dealing with the SAR. The controller will liaise with other controllers regarding the SAR, and as they see fit in terms of the extent of the response and any exceptional circumstances to limit the provision of information, that they may consider to be relevant.</p> <p>Additionally, myCMC Initiate and View functionality provide patients with direct access to view (and request changes to) their CMC care plan information.</p> <p>Note also that clinicians can print paper copies of CMC urgent care plans to give to patients from the CMC system at any time during care delivery and this is not dependent on a SAR.</p> <p>Yes. Firstly, where the ‘myCMC Initiate’ pathway on the patient portal is being used, while creating the CMC care plan request, the patient / data subject is effectively the data controller who controls the scope and accuracy of the data. At any time up to submitting their ‘myCMC Initiate’ request for a care plan to a doctor or nurse, the patient can cancel their request and the information that they had recorded is deleted.</p> <p>Once the patient has submitted their ‘myCMC Initiate request and the plan is added to and clinically approved, the patient / data subject can be enrolled to have a myCMC user account where they can view and request changes to their plan in the future.</p> <p>The patient / data subject can also subsequently withdraw consent to their CMC urgent care plan, indicating this to a clinician, which when executed, will put the care plan beyond use. A new care plan would need to be started again if the patient changed their mind at some future date.</p>

<p>How have you ensured that the right to data portability can be respected? Example: Data relating to particular people can be extracted for transfer to another Data Controller, at the request of the person to which it relates.</p>	<p>The myCMC patient portal is integrated with the CMC clinical system, which supports the CMC collaborative urgent care planning service across the 32 London CCGs.</p> <p>In the event that a patient / data subject transferred out of area or wished to move to another Data Controller of another platform, the CMC clinical system can be used to provide the patient's CMC care plan as either an electronic PDF or a printed document for transfer to another provider.</p>
<p>What confidentiality and security measures will be used to store the data?</p>	<p>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.</p> <p>These robust measures are defined by the Coordinate My Care Service Agreement between InterSystems and The Royal Marsden NHS Foundation Trust – the trust hosting the CMC service. These include but are not limited to:</p> <ul style="list-style-type: none"> • 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. • Royal Marsden Hospital Trust's IT Acceptable Use Policy and IT Security Policy conformance. • System Security Plan (SSP) provision, including a Data Protection approach. • Best practice Operational Security Plan for CMC system live operation.
<p>What security measures will be used to transfer the data?</p>	<p>The CMC IT solution is a collaborative, integrated system, with all care providers accessing a single, shared urgent care plan; data is not explicitly transferred outside the system. However, urgent care services are updated at a defined frequency with a secure file of additions, changes and removals of urgent care plans for patients for whom they provide services, so that CMC existence flags can be maintained.</p> <p>Clinician use of CMC: All user connections to CMC are by a secure network connection (Health and Social Care Network) – or via the internet using a 2 factor authentication method. All users access the system using a username and password or smartcard access</p> <p>The patient or their proxy access to myCMC is via a secure web link and is controlled by username and password. The myCMC patient portal is connected to the CMC system via a secure API (Application Programme Interface). Emails sent to NHS email addresses may include patient identifiable data. Emails sent to</p>

<p>What measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed on an authorised basis?</p>	<p>non-NHS email addresses exclude patient identifiable data or are encrypted.</p> <p>CMC has a comprehensive Information Governance policy, which must be adhered to by care organisations and staff accessing patient care plan data. Organisations using the CMC service must complete the CMC joint controllers Information Sharing Agreement (ISA). Organisations also complete User Access Forms (UAF), to request staff access to the CMC system, which includes submission of user training / competency in use of the CMC system.</p> <p>All users of the CMC solution will have completed annual data protection and cyber security training.</p> <p>Training is available in the form of a comprehensive set of eLearning modules, via Webinars, Face to Face or self-directed using our comprehensive PDFs of the e-Learning modules.</p> <p>Users must acknowledge the CMC Acceptable Use Policy (AUP) the first time they login to the CMC system and periodically thereafter.</p> <p>Individual users are assigned a username, password and role and also set up a security question and answer. Passwords expire automatically after 180 days of non-use. Role based access control is in place.</p> <p>Individual users must claim a Legitimate Relationship with a patient when they access their care plan initially.</p> <p>All CMC system events are audited. Audit information includes: date, time, event type, patient identification, user identification and organisation identification.</p> <p>In myCMC Initiate, the patient / data subject can either create the CMC care plan request in a single session or can do so in multiple sessions, stopping to resume at a later time. When resuming their care plan request, patients / data subjects must enter their NHS Number, a security passcode created when they began creating the request and a security token emailed to them together with the link to resume.</p> <p>Once submitted to the CMC system the patient's / data subject's care plan request can no longer be accessed via the myCMC patient portal.</p> <p>When the CMC care plan request has been accepted, consent has been confirmed, medical information has been added and the plan has been clinically approved, the data subject (and any nominated proxies) can be enrolled in myCMC, subject to authentication of their identity. Patients/ data subjects (and proxies) are emailed a link and activation code with which to activate their accounts; they are required to enter their NHS Number, Date of Birth and set up a myCMC username and password and define multiple security questions and answers. Patients / data subjects are then able to view and request</p>
---	---

	changes to their clinically approved care plan. All myCMC events are also audited.
--	---

Description of data flows

Has a data flow mapping exercise been undertaken? Yes

A data flow mapping exercise has been undertaken for the CMC IT solution, including myCMC. The RMH Data Mapping Tool CMC is attached below:

The collection, use and deletion of personal data should be described here. ***It would be useful to provide a flow diagram to illustrate the data flows.*** [Not yet available].

Does any data flow in identifiable form? If so, from where, and to where?	Yes. See associated Data Mapping Tool
Method of data flow? (e.g. email, fax, post, courier, other – please specify all that will be used)	See associated Data Mapping Tool

Reporting requirements by the project / processing

Are there any new or additional reporting requirements on personal data that is processed as a result of this project? Yes	
Indicate which roles will be able to run reports?	CMC Service Team members
Indicate which roles will receive the report or where will it be published?	CMC service users, typically team leads, those with management responsibility, CCG commissioners and transformation leads.
Will the reports include person-identifiable, pseudonymised or anonymised data?	Aggregated, non-person-identifiable data
Will the reports contain sensitive data or be redacted (removing anything which is sensitive)?	No
If this new/revised function should stop, what are the plans for how the information will be retained / archived/ transferred or disposed of?	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;”.

List of organisations involved in processing the data

Organisation Name	Organisation Role: Data controller/ Data Processor	Attained DSPT	Mandatory Training in place?			
			Data Collection	Use of System/ Service	Collecting patient sharing preferences/ consent	Information Governance/ Cyber security
Coordinate My Care	Data Processor	Yes	Yes	Yes	Yes	Yes
InterSystems	Data Processor	Yes	N/A	Yes	N/A	Yes
Health & Social Care Providers who have joint data controller Information Sharing Agreements with CMC These organisations are too numerous to list in this document. CMC has ISAs with over 1,650 organisations. Available on request from coordinatemycare@nhs.net	Data Controller	Yes	Yes	Yes	Yes	Yes

Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm Remote, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high
<p>1. Risk: A person maliciously creates a CMC urgent care plan request for another person via the myCMC Initiate facility within the patient portal myCMC. Mitigation: The urgent care plan must be completed during or after a patient’s appointment during which their identity is confirmed, their consent recorded, medical information added and clinical approval recorded.</p>	Possible(3)	Minimal(2)	Low (6)
<p>2. Risk: A person begins to engage with the CMC service, then subsequently discovers that they do not live in an area where the CMC service is commissioned. Mitigation: The commissioned area specific nature of the CMC service is highlighted in CMC communication materials. The initial question in the myCMC Initiate questionnaire is Postcode, which is used to check whether the patient lives in an area where the CMC service is available. Therefore patients do not waste their time completing the questionnaire only to discover that the service is not available to them.</p>	Remote (2)	Significant(3)	Low (6)
<p>3. Risk: A person could stop completing their myCMC Initiate questionnaire with the intention of resuming later but forget their passcode and is therefore unable to resume. Mitigation: The importance of remembering a passcode is highlighted when it is created and when pausing completion of the questionnaire with the intention of resuming at a later time. myCMC initiated questionnaires that have not been submitted but have been inactive for 60 days are automatically deleted. It is always possible for a person to restart the myCMC Initiate questionnaire from the beginning.</p>	Possible(3)	Minimal(2)	Low(6)
<p>4. Risk: There is a delay between a person submitting their myCMC request for a care plan and the request being completed by a doctor or</p>			

Authoring Department:	Information	Version Number:	{version number}
Author Title:	Information Governance Manager	Published Date:	{published date 78}
Ratified By:	IG Committee; IGRM	Review Date:	{review date 45678}
Uncontrolled if printed			

<p>nurse, being clinically approved and available to urgent care services. Mitigation: Guidance is provided to the patient that the onus is on them to initiate an appointment with their doctor or nurse to have their care plan completed. The CMC system includes workflow escalation to ensure that the task to complete the care plan is not overlooked.</p>	Possible(3)	Minimal(2)	Low(6)
<p>5. Risk: Failure to gain consent for care plan where patient is mentally competent to grant consent. Mitigation: The first screen of the care plan creation workflow is the consent section and it is not possible to move forward without inserting a value. CMC Communication materials highlight that CMC as an advance care plan is consent based, all training materials highlight when consent is required, the first screen for a new patient care plan starts with capturing evidence that the patient has consented. Professional codes highlight the importance of honesty and to not consent a patient and then record that they have consent would breach their professional code.</p>	Possible(3)	Minimal(2)	Low(6)
<p>6. Risk: Delay in processing patient's withdrawn consent so that the care plan is no longer available on the CMC care plan platform. Mitigation: There is a Withdrawal of Consent section on the CMC care plan which the patient's clinician can use to record the withdrawn consent and effectively remove the care plan from availability. Existence flags at the Urgent Care Services would then be automatically withdrawn. A new care plan could be created if the patient wished to have the support of a CMC care plan in the future. CMC have a protocol for withdrawing consent on the care plan if the CMC user asks CMC to withdraw the care plan from view as a result of the withdrawn consent.</p>	Possible(3)	Minimal(2)	Low(6)
<p>7. Risk: Inappropriate care plan access by a non-clinician picking up a mobile device which belongs to a clinician who uses it to access CMC. Mitigation: All CMC system access is by unique user name and password. Login sessions are automatically timed out after a period of inactivity reducing the likelihood of an unauthorised user gaining access to CMC data via a mobile device. CMC only allows access to CMC through non-personal mobile devices (owned by employer). CMC</p>			

Authoring Department:	Information	Version Number:	{version number}
Author Title:	Information Governance Manager	Published Date:	{published date 78}
Ratified By:	IG Committee; IGRM	Review Date:	{review date 45678}
Uncontrolled if printed			

<p>has a mobile device policy in place. Access to CMC would be via a two factor authentication method or a Citrix type remote access via their host employer network.</p> <p>8. Risk: CMC user deliberately looks at care plans which they have no legitimate need to.</p> <p>Mitigation: All accesses to CMC are audited. Any suspected breaches can be investigated. All users sign up to appropriate use of care plans and attend annual information governance training. Access by clinicians relies on clinician’s accountability to their professional body.</p>	Possible(3)	Minimal(2)	Low(6)
	Remote (2)	Minimal (2)	Low(4)

Identify Measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk Eliminated, reduced or accepted	Residual risk Low, medium or high	Measure approved Yes/no
None of the risks identified above has been identified as medium or high risk.				

Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Not applicable. None of the risks identified above has been identified as medium or high risk.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Not applicable. None of the risks identified above has been identified as medium or high risk.	If accepting any residual high risk, consult the ICO before going ahead

Authoring Department:	Information	Version Number:	{version number}
Author Title:	Information Governance Manager	Published Date:	{published date 78}
Ratified By:	IG Committee; IGRM	Review Date:	{review date 45678}
Uncontrolled if printed			

DPO advice provided:	Not applicable. None of the risks identified above has been identified as medium or high risk.	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Not applicable. None of the risks identified above has been identified as medium or high risk.		
DPO advice accepted or overruled by:	Not applicable. None of the risks identified above has been identified as medium or high risk.	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	Gerard Bowden, CMC Director of Nursing. Alan Ball, Information Governance Manager, The Royal Marsden NHS Foundation Trust.	

Overall Risk Rating

The overall risk rating is identified using the following risk matrix:

Likelihood		Actual Severity Consequence				
		None/ Insignificant	Low/ Minor	moderate	Severe/ Major	Death/ Catastrophic
		1	2	3	4	5
Almost Certain	5	yellow	yellow	orange	red	red
Likely	4	yellow	yellow	orange	red	red
Possible	3	green	yellow	orange	red	red
Unlikely	2	green	green	yellow	orange	red
Rare	1	green	green	yellow	orange	red

<END OF DPIA>

Please send this form to the Information Governance Manager for review.

***DPIA to be added to the DPIA log, updated on the Trust website and bi-monthly report sent to the Caldicott Guardian and SIRO.**

[End of Document - Do Not Delete]



RMH Data Mapping
Tool

Authoring Department:	Information	Version Number:	{version number}
Author Title:	Information Governance Manager	Published Date:	{published date 78}
Ratified By:	IG Committee; IGRM	Review Date:	{review date 45678}
Uncontrolled if printed			