coordinate
my care
Urgent Care Plan

PRIVACY IMPACT ASSESSMENT FOR Coordinate My Care

Version Control

Version Number	Amendments made	Changes made by	Date
2.0	Corrections, reformatting, Appendices 2-4	Coordinate My Care IT Architect	18th January 2013
2.1	Further minor amendments following RMH IG Lead review	Coordinate My Care IT Architect	23rd January 2013
2.2	Clarify use of Patient Information Leaflet Clarify data retention policy Further minor amendments	Coordinate My Care IT Architect	28th January 2013
2.3	Updates to reflect recent SPICT changes Reflect potential role of Lasting Power of Attorney for Personal Welfare in consent process Refer to CMC Data Quality Processes Separate original from current stakeholder groups Coverage of social services involvement Remove references to London Coverage of non-N3 connectivity Reflect implemented CMC data retention and 'hard deletion' capabilities Reflect tape encryption now in place Remove requirement for 2 health care professionals to be involved in CMC decision Reflect Urgent Care service CMC existence flagging Further minor amendments	Coordinate My Care Nurse Manager Coordinate My Care IT Architect	14th February 2014
3.0	Further minor amendments	Coordinate My Care Nurse Manager Coordinate My Care IT Architect	27th March 2014
4.0	Modify to reflect use of CMC by social care professionals Modify to reflect use of CMC with children Modify to reflect use of CMC with patients who require personalised urgent care plans but who are not within their last 12 months of life Modify to clarify consent options Review and update DPA Compliance Checklist (Appendix 4) List additional Patient Risks in Risk Assessment Formatting improvements, minor corrections and clarifications	Coordinate My Care Director of Nursing Coordinate My Care IT Architect	26th February 2015

Contents

Objectives and Scope of this Document

Aims of Privacy Impact Assessment (taken from ICO website):

- ensure effective management of the privacy impacts arising from the project;
- ensure effective management of the project risks arising from the project's privacy impacts; and
- avoid expensive re-work and retro-fitting of features, by discovering issues early, devising solutions at an early stage in the project life-cycle, and ensuring that they are implemented

Privacy risks fall into two categories:

i) Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information.

ii) Risks to the organisation as a result of:

- perceived harm to privacy;
- a failure to meet public expectations on the protection of personal information;
- retrospective imposition of regulatory conditions;
- low adoption rates or poor participation in the scheme from both the public and partner organisations;
- the costs of redesigning the system or retro-fitting solutions;
- collapse of a project or completed system;
- withdrawal of support from key supporting organisations due to perceived privacy harms; and/or
- failure to comply with the law, leading to enforcement action from the regulator, or to compensation claims from individuals.

This document includes:

1) List of stakeholders
2) Project aims, current standards, and product description
3) Scope and process mapping for the project
4) Foreseen risks prior to stakeholder engagement
5) Screening Analysis (Appendices 1, 2, 3)

These five sections reflect the formal Privacy Impact Assessment undertaken at initiation of Coordinate My Care in 2012, annotated as necessary to reflect the current CMC environment and current CMC practice.

6) Data protection compliance check (Appendix 4)

This section reflects the current CMC environment and current CMC practice.

7) Outstanding areas of the PIA are:External Assessment – consultation and information gathering
8) Internal Analysis
9) Documentation
10) Privacy law compliance check

CMC is currently developing an Action Plan to deliver these.

Coordinate My Care is currently working to re-platform the CMC System. This work will include a refreshed Privacy Impact Assessment, updating the information provided here. CMC's Communications Strategy for implementation of the new system will disseminate relevant information as necessary.

CMC Initiative Privacy Impact Assessment (2012)

Stakeholders

The following is a list of those involved in the original Privacy Impact Assessment carried out in 2012:

Julia Riley - Consultant Royal Marsden Hospital
Stephen Elgar - IG Manager NHS London
Eileen Sutton - 111 lead NHS London
Libby Hough - Development Manager CMC
Dr Chi Chi Cheung - IG clinical lead CMC
Matthew Nye - IT Lead for NHS London 111 project
David Whitmore - Clinical lead to Medical Director, LAS
Jackie Harris - End of Life Project, Connecting for Health
Phil Koczan - GP NHS London
Marlene Winfield - Carer representative

A list of current Project Steering group members can be obtained on request from coordinatemycare@nhs.net.

Aims

Coordinate My Care provides an electronic Personalised Urgent Care Plan.

The overriding aim is to improve identification and communication of information between health and social care providers in all settings for end of life care and other potentially benefiting patients to enable patient preferences to be achieved.

More specific aims of the initiative relate to:

- To identify more patients approaching the end of life across all diagnoses
- To enable other patients who may benefit from a personalised urgent care plan to have one put in place
- To discuss preferences and wishes with a higher proportion of these patients and record the outcome of discussions in a shareable format
- To have a mechanism by which all urgent care services are alerted to the existence of personalised urgent care plans for these patients, and which gives these services access to up to date information
- To reduce inappropriate hospital admissions and length of stay for end of life patients
- To appropriately increase the number of patients at the end of life with a Do Not Attempt Cardio-Pulmonary Resuscitation (DNACPR) order in place
- To increase the number of patients who have their preferred place of care and death documented
- To increase the number of patients who achieve their preferred place of care and death

Standards

Coordinate My Care works closely with NHS England concerning standards both for Urgent and Emergency Care and for Electronic Palliative Care Coordination System (EPaCCS).

The CMC care plan conforms with the ISB1580 standard in relation to End of Life Care.

Product Description

The product is an electronic web accessed software package to store and communicate end of life and other personalised urgent care plan patient information between health and social care providers across all settings and in both statutory and voluntary sectors: general practice, acute (including A&E), community, mental health, out of hours GPs, 111, ambulance services, hospices, care homes, social services.

Scope and Process mapping

For the purposes of this initiative and because of the risks of inappropriately identifying patients as end of life the following inclusion criteria were originally in place:

- Patients will need to meet the following criteria to be considered for a CMC personalized urgent care plan:
    - i) Age over 18 years
    - ii) Life limiting illness
    - iii) At risk of deteriorating and potentially dying
- Agreement amongst the health professionals involved in the care of the patient that the patient has this prognosis

Any change to, or expansion of, CMC's remit is controlled through the CMC Steering Group and the CMC Governance Board. A list of current members of these bodies can be obtained on request from coordinatemycare@nhs.net.

CMC now also stores and coordinates personalized urgent care plans for a wide range of patients who, while not meeting the above criteria, are judged by the professional(s) responsible for their care as potentially benefiting from a personalized care plan. In many cases, but not exclusively, such identification is consequent on the patient's meeting the criteria of an initiative such as Avoiding Unplanned Admissions.

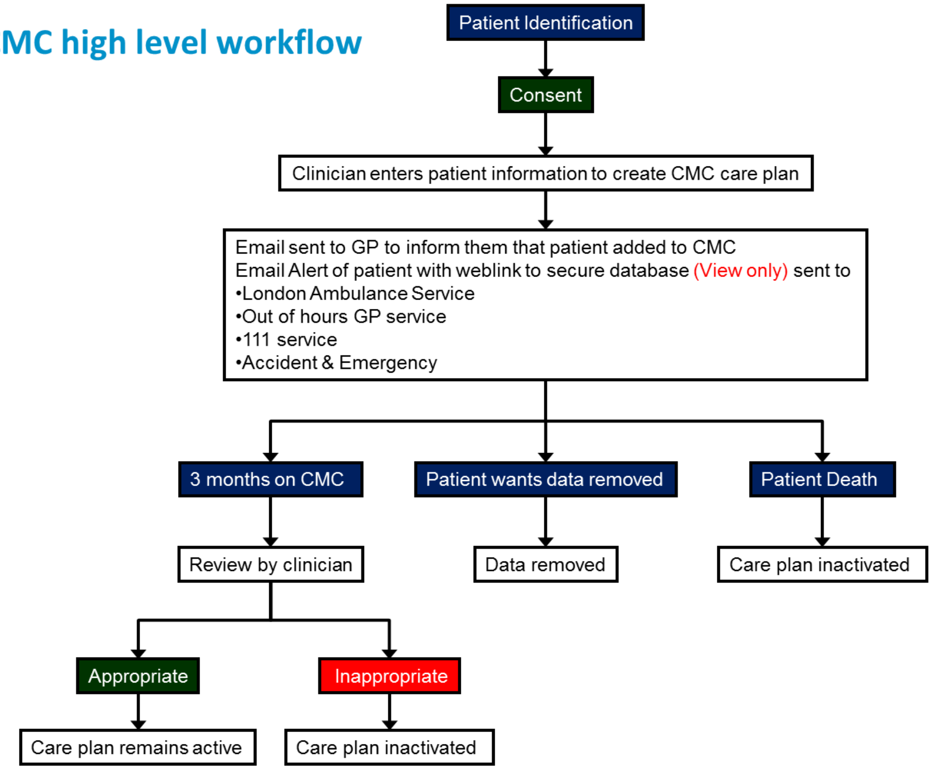
Those under 18 are now also covered by CMC.

The name of the system is 'Coordinate My Care' (CMC).

- CMC will involve health and social care professionals identifying patients they think are at the end of life, or who would otherwise benefit from a personalized urgent care plan (as just discussed).
- The patient can have any diagnosis (so not cancer exclusive).
- The health professional will then consent the patient (or in some cases, for those under 18, the patient's legal guardian) to have their information shared with other professionals (Out of hours GP (OOH GP), London Ambulance Service (LAS), Community Palliative Care team, GP, etc.).
- This will include a discussion, if this has not already occurred and if it is appropriate, about prognosis and patient preferences regarding place of care and death.
- The information held will include diagnosis, treatment, prognosis, resuscitation status, medications, carer, community and hospital team demographics, social services support information, and preferred place of care and death if known.
- As part of the consenting process the patient will be offered a paper copy of their information held on CMC. This will be generated from the software after details have been inputted by the care professional and given to the patient. It will act as a check that the correct information has been inputted; patients will be able to contact the care professional who inputted their details if there are any alterations required.
- 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, the professional must either refer to the patient's Lasting Power of Attorney for Personal Welfare, or make an informed decision in the patient's best interests, in accordance with the Mental Capacity Act 2005 and with normal clinical practice.

CMC can be accessed by a health or social care provider from a web browser with either N3 or non-N3 connectivity (please refer to the Coordinate My Care System Level Security Policy for details). The clinician is able to update any changes to the patient's care plan directly and this is then viewable by all professionals involved in their care. Once a patient dies, their care plan will be deactivated by the appropriate user that has editing rights.

CMC high level workflow



Patient Identification

Consent

Clinician enters patient information to create CMC care plan

Email sent to GP to inform them that patient added to CMC
Email Alert of patient with weblink to secure database (View only) sent to
•London Ambulance Service
•Out of hours GP service
•111 service
•Accident & Emergency

3 months on CMC

Patient wants data removed

Patient Death

Review by clinician

Data removed

Care plan inactivated

Appropriate

Inappropriate

Care plan remains active

Care plan inactivated

CMC Initiative Risk Assessment (2012)

Foreseen risks before embarking on Stakeholder engagement

This risk management plan was developed after consultation with members of the RMH palliative care team, and the lead clinician of the Camden and Islington End of life register pilot.

Note that at that time CMC's coverage was limited to End of Life Care patients aged 18 and over, while its usage was limited to health care professionals. However CMC feels that this risk management plan remains applicable (notes in [square brackets] have been added where relevant).

The risk management plan has been divided into the following risk categories:
(1) Set up
(2) Implementation
(3) Patient risks
(4) Information Governance/Privacy
(5) Staff risk
(6) Trust/DOH risks

Set up risks

(a) Difficulty engaging health care professional

- Role of CMC Director of Nursing and facilitators will be an education programme delivered to all professionals involved in the care of patients in each locality to encourage the use of End of Life Care tools
- Use of CQIN and LES to encourage the uptake of CMC where agreed and funded in the localities

(b) Delay in database set up

- [System has successfully been live (post-pilot) since April 2012.]

Implementation

(a) GP lack skills or are concerned that they lack the skills to have the necessary conversations with patients

- Part of the GP training will focus on Breaking Bad News and end of life discussions.
- If felt valuable to GP's then a script or guidance phrases will be provided
    - This is particularly important around whether to discuss resuscitation

(b) Oncologist or other specialist doctors reluctant to label one of their patients end of life, and reluctant to give a prognosis as too difficult to predict.
Educational events/grand rounds about the purpose of the personalised care plan.

[CMC personalized urgent care plans are no longer limited to End of Life Care patients.]

Patient risks

(a) Wrongly identified as end of life and therefore clinically mismanaged

- Whether the patient is appropriate to the CMC process has to be a clinical decision taken by the health care professionals directly involved in that patient's care. The consent of the patient is required, except in cases (as above) where the patient lacks mental capacity as defined under the Mental Capacity Act 2005, in which case staff are encouraged to involve the family/carer(s)
- The CMC process is limited to end-of-life care for patients considered to be at risk of deteriorating and potentially dying. Please see the 'Identity' section of Appendix 1 below for further information on the criteria used [but note that CMC personalized urgent care plans are now no longer limited to End of Life Care patients]
- The CMC care plan does not replace clinical decision making at the point of care

[*(b) Patient has CMC care plan created but GP specified on care plan does not have access to the system, or patient is outside CMC coverage area*

- CMC monitors for patients in these categories and communicates with the care plan creator and/or GP surgery as appropriate to the circumstances, arranging CMC training for the latter as necessary.

(c) Urgent Care service clinician not aware of CMC care plan because of (manual) urgent care service system flagging backlog, e.g. over weekend

- CMC has an initiative in place to deploy automated flagging to all urgent care services.
- Manual flagging, where still necessary, needs to be resourced appropriately by urgent care services.
- CMC works with urgent care services to ensure that the impact of such a backlog is understood.

(d) Following extension of CMC remit to cover non End of Life care plans: such patients might be inappropriately treated with palliative intent

- Appropriate communication to all relevant care providers when extended CMC coverage is initiated in a specific CCG.
- Wording of urgent care service system flags amended to remove references to End of Life.
- Users are taught to always check a patient's CMC care plan rather than make assumptions.]

Information Governance

(a) Confidentiality

- Only professionals with logon details are able to access CMC
- Professionals may only obtain logon details once they have received formal training/awareness of Coordinate My Care and of the CMC computer system, and have signed a detailed Acceptable Use Policy
- There is a complete audit trail of all activity on CMC
- User has to declare a legitimate relationship with patient before being able to view their care plan on CMC
- There will be regular monitoring of user access to the CMC System

(b) Not all Health Care Professionals and Allied Health Professionals have access

- Non-N3 solution is now available, so there is no technical barrier to take-up of CMC
- CMC has a communications strategy which will ensure that the whole end of life care network [and other stakeholders] are aware of CMC

(c) Information entered onto the register incorrectly (may lead to inappropriate clinical care)

- At consent the patient, or relative if the patient lacks capacity, will be offered a paper copy of the register information. The patient information leaflet states that this is also a way in which they can check their details are correct
- Random sampling of a proportion of the database will be done at regular intervals, and the database entry fields checked

[CMC has detailed Clinical Safety and Data Quality processes in place, managed by a dedicated Clinical Quality Manager.]

(d) *Security*

- Please refer to the Coordinate My Care System Level Security Policy

Staff risks

(a) Accident or injury occurs involving a member of RMH staff whilst visiting other trusts, GP practices or Hospice units (for example accidents involving transport/travel)

- RMH staff will always contact other team members on leaving the trust and comply with the CMC Lone Worker Policy
- RMH staff will adhere to existing incident and accident policies and procedures

Trust/DOH risks

(a) Complaint made by other Health Care Professionals, or by patients

- Any of the above occur and as a result of a complaint about the CMC process the trust is required to pay compensation to individuals and significant damage is done to the trust's reputation
  - A great amount of time has been spent with stakeholders, this should include the patient/carer group
- A number of pilots have problems because this is a very sensitive issue in vulnerable patients, resulting in a complaint to the Department of Health
  - Steering group of all live sites meet regularly to ensure risks are shared and minimized

Appendix 1: Criteria for small-scale PIA (initially completed 2012)

Technology

(1) Does the project involve new or inherently privacy-invasive technologies?

Coordinate My Care does not involve any new or inherently privacy-invasive technologies.

It is an electronic method of holding patient information and details to be accessed only by health and social care professionals when caring for the patient. It does not involve any intrusive technologies such as surveillance, and all the information held on the care plan will have been put there with the patient's consent.

It is a web based software solution (System C) based on the PROTOCOL software package already used in social services across the UK.

The idea of sharing patient information electronically across different health care settings and providers is not new in health care; it is occurring in other places in the country, has occurred through paper handover within Sutton and Merton and the premise is the same as that of the Summary Care Record.

In summary, no, the project does not involve new or inherently privacy-invasive technologies

Justification

(2) Is the justification for the new data-handling unclear or unpublished?

The loss of privacy for this project is with the patient's consent or endorsement of the family members, and is only done to benefit the patient. The benefits of holding the patient's information on an electronic record such as this is that currently although individuals may be on a register at their GP practice, this information as it is updated is not shared with other health professionals, specifically out of hours GPs, 111, the local A&E, and the Ambulance service. Out of hours teams contribute to the majority of patient care and keeping them informed about the patient's condition, wishes and preferences will benefit patients through realizing their preferences.

In summary, the justification for this project is clear.

Identity

(3) Does the project involve an additional use of an existing identifier?

The existing identifier used in the community for patients approaching the end of life is from the SPICT tool (NHS Lothian) to identify EoLC patients.

The identifier for entering patients on CMC from an End of Life Care perspective is:

Look for two or more general indicators of deteriorating health:

- Performance status poor or deteriorating, with limited reversibility (needs help with personal care, in bed or chair for 50% or more of the day)
- Two or more unplanned hospital admissions in the past 6 months
- Weight loss (5-10%) over the last 3-6 months and/or body mass index<20.
- Persistent troublesome symptoms despite optimal treatment of any underlying condition(s)
- Lives in a nursing home or NHS continuing care unit, or needs care to remain at home
- Patient requesting supportive and palliative care, or treatment withdrawal.

This was chosen to ensure patients are not inappropriately added to CMC.

The other patient identifiers in use in this project are the same as those already in use; the NHS number and date of birth.

Identifiers relating to non-End of Life Care usage of CMC will be added to this section as they arise.

(4) Does the project involve use of a new identifier for multiple purposes?

No

(5) Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?

Patients who would be appropriate for CMC are:

- those approaching the end of life (any diagnosis) - these patients should have already been identified by health professionals, as part of the Gold Standard Framework/SPICT;
- those who, while not meeting end of life criteria, are judged in the course of their care as potentially benefiting from a personalized care plan (in many cases, but not exclusively, such identification is consequent on the patient's meeting the criteria of a separate initiative such as Avoiding Unplanned Admissions).

CMC is an electronic method of collating this data and communicating it with other health professionals and with social care professionals. There is no intrusive or onerous change of identification authentication process.

Data

(6) Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?

The project may result in handling new data about patients, as the existence of CMC may encourage/remind health and social care professionals to discuss a personalised urgent care plan with patients and therefore generate new data surrounding preferences, care planning etc. This will only be stored on CMC with the patient's consent.

The data will be held on a new software database (System C), and so this is a significant change to how this information is stored currently within London, although similar projects are already running elsewhere in the country (Weston PCT).

The project is intended to amount to a small amount of extra data holding to improve care.

(7) Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?

No

(8) Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?

Data will be sourced from the patient/ care professional interaction and only updated or changed via this method. The patient will therefore be fully aware of the information held about them.

The use of CMC by Urgent Care services is dependent on the placing and maintenance of CMC existence flags on Urgent Care systems. These flags contain no CMC data, purely an indication of existence of a CMC care plan.

Data handling

(9) Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?

Data collection policy will remain the same; the storage of the data is on a new database.

(10) Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?

Information on CMC's Data Quality Processes is available on request to coordinatemycare@nhs.net.

(11) Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?

The data security is clear.

The data security for this project will take two forms; the patient will be aware of the weblink to their electronic information and can inform health and social care professionals to view it – thereby giving their consent to view. Secondly, the CMC application is password protected, and this is auditable.

(12) Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?

No, data access and disclosure is clear and traceable.

Previously within London if a patient was recognized as end of life the relevant OOH GP service and Ambulance service were informed about the patient, given information pertaining to the end of life and patient preferences only, via a fax and this was stored at both headquarters on their computer systems. The new process will involve the information being accessed via a secure web browser based application, which can be audited to determine who accessed the care plan and when. On access only individual patient information will be viewable. The data will be accessed by three extra groups of staff compared to previously: the CMC (for audit purposes), A&E, and 111 service staff.

This will be explained in the patient information sheet.

(13) Does the project involve new or changed data retention arrangements that may be unclear or extensive?

The data will be stored on a new database specifically designed for storage of personalised urgent care plan information. The software decided on (System C) is currently used in social services locations across England.

This is a change, but is not extensive. The data will be managed according to the Royal Marsden's data retention and disposal policy (which has a standard data retention period of 30 years).

(14) Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

No, data is not publicly available.

<u>Exemptions</u>

(15) Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?

No.

Appendix 2: Section A: New/Change of System/Project General Details

Project/System Name	Coordinate My Care	
Objective/Purpose	Please refer to body of PIA	
Background: Why is the new system / change in system required?	Please refer to body of PIA	
Benefits (if relevant)	Please refer to body of PIA	
Date of completion	Version 1: 24 April 2012 Version 2: 18 January 2013 Version 3: 27 March 2014	
Name of assessor	**Job Title**	Mandy Shaw, IT Architect, Coordinate My Care
	Department/Office Base	
	Phone	
	Email	
Information Asset Owner: (All systems/assets must have an Information Asset Owner (IAO). (IAOs are normally the Trust Directors with overall responsibility for the service/database)	**Job Title**	Chief Nurse, Royal Marsden
	Department/Office Base	
	Phone	
	Email	

Appendix 3: Section B: Privacy Impact Assessment Key Questions

Identity	Is this information identifiable to the individual?	Yes
	If YES what sort of personal data is identifiable? If OTHER please specify	Please refer to section 3.1 of the Coordinate My Care Information Sharing Agreement, which provides a full list.

Category	PIA Check	Yes/No
3rd Party Supplier	If relevant does the third party/supplier contract contain all the necessary Information Governance clauses including information about Data Protection and Freedom of Information?	Yes
Technology	Does the project apply new or additional information technologies that have substantial potential for privacy intrusion? *Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS)*	See Appendix 1 question 1 NHS smartcards may be used to access the CMC system, but only when an underlying and active CMC userid and password is in place.
Data Handling / Data Sharing	Will the project/system result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?	See Appendix 1 question 6
	Does the project involve systematic disclosure of personal data to other NHS organisations?	Yes, this is central to the objectives of the project
	Does the project/system involve new or changed data *collection* policies or practices that may be unclear or intrusive?	See Appendix 1 question 9
	Does the project/system involve new or changed data *quality/security* assurance processes and standards that may be unclear or unsatisfactory?	See Appendix 1 questions 10 and 11
	Does the project/system involve transfer/storage of Personal Identifiable Data (PID) outside the European Economic Area (EEA)?	No
	Does the project/system involve the systematic disclosure of PID to private sector organisations (e.g. as outsourced service providers or as 'business partners')?	Yes, e.g. Out of Hours providers, private sector Nursing Homes
	Does the project involve sharing with multiple organisations, whether they are government/NHS agencies or not (e.g. in 'joined-up government' initiatives)?	Yes, this is central to the objectives of the project

	Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?	See Appendix 1 question 8

Appendix 4: Section C: Data Protection Compliance Checklist

1. What type of personal data are you processing (staff/patient) and who are the intended primary users?

Please refer to section 3.1 of the Coordinate My Care Information Sharing Agreement for details of the data being processed.
Primary users are participating organisations' care professionals and clinical/social care administrative staff.

Schedule 2 - Grounds for Legitimate Processing of Any Personal Data

2. Have you identified all the categories of personal data that you will be processing and how? Yes

3. If yes, please list them (e.g. name, DOB, address, NHS Number). If no, please indicate why not.

Please refer to section 3.1 of the Coordinate My Care Information Sharing Agreement for details of the data being processed.

Obtaining consent

(Please note that patient consent is only required where the primary purpose is not for the treatment, diagnosis of patients or for assessing the quality of healthcare via clinical audit)

4. Are you relying on the individual to provide consent to the processing of their personal information? 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 must refer to the patient's Lasting Power of Attorney for Personal Welfare, or make an informed decision in the patient's best interests, in accordance with the Mental Capacity Act 2005 and with normal clinical practice.

5. If yes, when and how will that consent obtained?

Consent is obtained at the beginning of the CMC patient registration process and is recorded by being entered on the CMC Care Plan.

Consent options are as follows:

For patients aged 18 years or older:

- The patient has agreed to the creation of a personalised care plan, and sharing of information as above
- The patient lacks the mental capacity to make these decisions, but consent has been given by an appointed person with Lasting Power of Attorney for personal welfare
- The patient lacks the mental capacity to make these decisions, but a clinical decision has been made in their best interest in consultation with family/carers
- Consent previously given, but now withdrawn [care professionals no longer have access to the care plan]

For patients aged 17 years or younger:

- The patient's parent/legal guardian has agreed to the creation of a personalised care plan, and the sharing of information as above
- The patient is aged 16 or 17 years, and has given their own consent
- The patient is aged 15 years or under, but was judged to have the capacity to give their own consent
- It has not been possible to obtain the consent of the patient's parent/legal guardian, but a clinical decision has been made in their best interest
- Consent previously given, but now withdrawn [care professionals no longer have access to the care plan]

6. Does the project involve the use of existing personal data for new purposes other than for the diagnosis, treatment, care of a patient or for clinical audit work? No

7. If yes, please describe:

Not applicable

Adequacy and relevance of Personal Data

8. How is an assessment made as to the relevance (i.e. no more personal information than the minimum required to perform the service) of personal data for the purpose for which it is collected?

The CMC Care Plan contains only the information essential to understanding and delivering the current and advance care needs and plans of patients who have been identified as end of life, and the information essential to accurate identification of the CMC Care Plan for a specific patient.

9. What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?

All CMC enhancements and modifications are subject to Change Control including review by the CMC Information Asset Administrator.

10. Are there procedures for assessing the amount and type of personal data collected for a particular purpose? Yes

11. If yes, please describe. If no, please indicate why not.

As CMC involves information sharing, the Coordinate My Care Information Sharing Agreement is considered the appropriate vehicle for storing and maintaining this information.

Accuracy of Personal Data

12. How, and how often, are personal data be checked for accuracy?

Please refer to Appendix 1 section 10.

13. In what circumstances is the accuracy of the personal data being checked with the Data Subject?

The personal data is reviewed with the Data Subject when the CMC Care Plan is created, and the Data Subject is at that time also offered a hardcopy of the completed CMC Care Plan.
The care plan includes a 'next review' date; the length of time before the next review is a clinical decision, but the default is 3 months.

Keeping Personal Data Up to Date

14. Are there procedures to determine when and how often personal data requires updating?

CMC requires periodic review of care plans for accuracy. The interval between such reviews defaults to 3 months but is a clinical decision.

Not kept for Longer than Necessary

15. Is there a retention period (the minimum timescale) for the personal data?

The retention period used is the Royal Marsden standard of 30 years. This starts when the patient care plan is closed, either because the patient has died or because the care plan is no longer required (the patient has withdrawn consent, or there has been a clinical decision to remove the patient from the CMC process). If the care plan is no longer required, it will be 'soft deleted' from the system.

16. When data is no longer necessary for the purposes for which it was collected:

    a. How is a review made to determine whether the data should be deleted? Please refer to the Phase One flowchart in section 3 of this PIA.
    b. How often is the review to be conducted? Every three months.
    c. Do you need to keep information to counter legal claims or for audit and inspection purposes? Yes (this is why 'soft deletion' is used, as above)
    d. If the data is held on a computer, does the application include a facility to flag records for review/deletion?

The application contains a facility to flag care plans for deletion (i.e. to 'soft delete' a care plan), but not for review.

17. Are there any exceptional circumstances for retaining certain data for longer than the normal period (e.g. for research purposes)? Potentially, although details of this are yet to be defined.

18. If yes, please give justification:

Not yet determined.

Rectification, Blocking, Erasure and Destruction

19. What is the procedure for responding to a request either from an individual or a court order requiring correction, erasure or destruction of personal data?

Each CMC care plan is the responsibility (as joint Data Controller) of its creating CMC user organisation, which will handle such requests according to its relevant internal procedures. At a technical level, data 'hard' deletion requests can be submitted through the CMC application.

Principle 7: Data Security

20. Is there a specific Security Management Policy and access policy in place?

Please refer to the Coordinate My Care System Level Security Policy.

21. Who will have access to the information (staff groups)?

1) Coordinate My Care user organisations’ care professionals and clinical/social care administrative staff as listed on the relevant User Access Forms
2) The CMC and Information Teams within the Royal Marsden
3) Liquidlogic, System C and McKesson staff for support purposes where necessary
4)

22. If known how does the level of security compare to industry standards, if any?

The Coordinate My Care System and its hosting conform to ISO27001.

Unauthorised or unlawful processing of data

Everyone in the Trust must safeguard the integrity, confidentiality, and availability of sensitive information. No one from the Trust – (this includes staff employed by commercial partners and volunteer groups) – should be sharing any patient sensitive information unless it can be justified on a need to know basis.

23. Describe security measures that are in place to prevent any unauthorised or unlawful processing of:

a. Data held in an automated format (e.g. password controlled access and/or role based access control)?

Please refer to the Coordinate My Care System Level Security Policy.

b. Data held in a manual record (e.g. locked filing cabinets)?

Not applicable

24. Describe the procedures in place to detect breaches of security? (E.g. audit?)

The Coordinate My Care Application has full audit trail functionality in place. This is available on a real-time basis to the CMC Administration team within the Royal Marsden.

25. Is there a useable audit trail in place for the asset? For example, to identify who has accessed a record?

The Coordinate My Care Application has full audit trail functionality in place. This is available on a real-time basis to the CMC Administration team within the Royal Marsden.

When members of the Trust are authorised to disclose identifiable information to other organisations outside the NHS, they must seek an assurance that these organisations have a designated safe haven point for receiving personal information. Any person-identifiable documentation must be addressed and sent to the intended recipient securely

26. If the data is sent outside of the Trust how the data will be sent/accessed and secured?

	Yes/No		Yes/No
Fax	Yes	Email	Yes
Via NHSMail	Yes	Via Courier	No
By hand	No	Via Post – Internal	No
Via Telephone	No	Via Post – External	No
Website	Yes		

Other – Please State Below:

CMC data is not duplicated or transferred: it is stored as a single instance and accessed by all users via the same browser-based CMC application (see https://protocolrm.syhapp.thirdparty.nhs.uk/).

A detailed list of CMC information flows will be found in section 5.4 of the CMC Information Sharing Agreement.

The following rules are in place in relation to faxes:

Incoming faxes:

A fax machine used to receive CMC person identifiable or sensitive information should be located in a physically secure environment; fax machines in non-secure localities must require the inputting of a PIN before they will print out a stored fax. Additionally, the fax should be removed from the machine on receipt and appropriately dealt with and safely stored. The sender must be contacted to confirm receipt.

Outgoing faxes:

Where CMC information is being faxed out, the sender should always contact the recipient after sending to ensure that the fax has arrived. Where such a fax is not part of a standard process, the recipient should also be contacted before sending, to ensure that the fax can be handled promptly and appropriately. The target fax number should be provided with a short code on the fax machine, to avoid mis-keying. All such faxes should be marked confidential with wording indicating that the fax must be destroyed if received by the wrong service. In addition the number of pages should be specified. There should also be a contact number to let the sender know if it is received in the wrong place.

27. Where will the information be kept/stored/accessed (e.g. on paper/on a database/on a network drive/website/ dedicated system/other)?

The data is kept in a database hosted by McKesson at their Warwick and Newcastle data centres. Please refer to the Coordinate My Care System Level Security Policy for more information.

Destruction of Personal Data

28. Describe the procedures in place to ensure the destruction of personal data no longer necessary?

CMC care plans will automatically be purged (hard deleted) from the CMC System once the end of their 30-year retention period has been reached, or if a ‘hard deletion’ mandate is received in relation to an individual care plan as discussed in section 19 above.

Contingency Planning - Accidental loss, destruction, damage to personal data

29. Is there a contingency plan to manage the effect(s) of an unforeseen event?

Yes

30. Describe the risk management procedures to recover data (both automated and manual) which may be damaged/lost through human error, computer virus, network failure, theft, fire, flood, other disaster.

Please refer to the Coordinate My Care System Level Security Policy and theCoordinate My Care Business Continuity Plan.

31. Is there a contingency plan / backup policy in place to manage the effect of an unforeseen event? Please provide a copy.

Yes – please see the Coordinate My Care Business Continuity Plan.

32. Has an information risk assessment been carried out and reported to the Information Asset Owner (IAO)? If so were any risks highlighted? Please provide details

Identified risks are as follows.

Major:

1) Hosting organisation not encrypting backup tapes sent off site. This was fully remediated by 1 March 2013.
2) Personally identifiable data that is no longer required for storage being hidden, rather than being deleted as required under the DPA 1998. This was fully remediated on 17 December 2013.
3) Initially data was checked for accuracy only ad hoc by clinicians accessing a specific CMC Care Plan in the course of care. Also, because the NHS number is not currently mandatory in CMC, there is no common key between CMC and other systems with which it needs to interoperate as described in section 26 above. The Coordinate My Care Team has since mid 2013 had proactive Data Quality measures in place such as reconciliation of CMC data against the Spine, with defined remediation procedures for exceptions detected. Also, the CMC System has had Spine integration for smartcard users since 17 December 2013.
   The new CMC system will make the NHS number mandatory and will extend Spine integration to all users.

Minor:

4) Many CMC users do not have nhs.net email addresses, and many CMC user organisations are unable to resource central distribution of logon information. This is now fully remediated through NHSMail’s capability, introduced in 2015, to distribute information securely to non-NHSMail recipients. See the CMC System Level Security Policy for details.
5) Following CMC application timeout, although the application cannot be used further until the user has logged in again, CMC data is still visible in the browser window. This is mitigated by the CfH IG Toolkit’s requirement that all relevant devices have operating system level screen lock timeouts in place. The new CMC system will fully remediate this risk.
6) CMC user organisations permitting use of the CMC application from mobile devices without formally agreeing to the CMC Mobile Device policy (because this had not been put in place when they signed the CMC Information Sharing Agreement). This will be addressed by the next re-distribution of CMC IG documentation to Data Controllers (April/May 2015).

This section is to be completed if personal data is being transferred to a country or territory outside of the European Economic Area

33. Are you transferring personal data to a country or territory outside of the EEA? No

34. If yes, where?

Not applicable

35. What is the data to be transferred to the non EEA country?

Not applicable

36. Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?

Not applicable

37. Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?

Not applicable

Data Protection Compliance

38. Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the checklist. This could include indicating whether some changes or refinements to the project might be warranted

The CMC Project is in our view currently compliant with this checklist, with the exception of the still not fully mitigated Major matter listed as a known risk in section 32 above:

- There is no common key between CMC and other systems with which it needs to interoperate as described in section 26 above.

Evaluation

39. Is the PIA approved? Yes

40. If not state the reasons why?