SYSTEM LEVEL SECURITY POLICY:

COORDINATE MY CARE

Document Version: **1.1**

Date: **25th February 2015**

Review: **December 2015**

Author: **Mandy Shaw, IT Architect, Coordinate My Care**

Approved: ***TBC***

DOCUMENT CONTROL AND AMENDMENT RECORD

NOTE: This is a CONTROLLED document. The current version of this document is maintained and is always available electronically via the Royal Marsden Hospital's secure Intranet. All other electronic or paper versions of this document sourced from any network drive, email or other sources are uncontrolled and should be checked against the current Intranet version prior to use.

Draft Version Control

Version	Date	Detail	Authors	Approval
0.1	26 Nov 2012	New Policy	Mandy Shaw	

Amendment Record

Version	Date	Detail	Author	Approval
0.2	12 Dec 2012	Amendments following initial review by RMH governance, and incorporating additional information received from managed service provider	Mandy Shaw	
0.3	13 Dec 2012	Minor amendments	Mandy Shaw	
0.4	19 Dec 2012	Minor amendments	Syma Dawson and Mandy Shaw	
0.5	20 Dec 2012	Initial released version	Syma Dawson and Mandy Shaw	Information Governance in RMH and in other CMC user organisations
0.6	13 February 2014	Addition of diagrams re CMC IG Pathway and re non-N3 access Modified user logon distribution mechanism Correct description of data warehouse data feeds Clarification of mobile device situation Tape backups now fully encrypted Coverage of non-N3 access to CMC Coverage of PDS integration Coverage of automated flagging Coverage of smartcard use Remove references to London Add faxing information Clarify rules re printing/storage of CMC operational report data	Mandy Shaw	

1.0	5 March 2014	Correction to user login distribution mechanism Correction to password policy Clarify situation re IG training Define 'DR' at first usage	Mandy Shaw	
1.1	25 February 2015	Clarify training requirement for read-only users Rewrite audit section to reflect the fact that CMC data is not controlled by RMH except where care plans are created or maintained by RMH staff Simplification of user logon distribution mechanism following introduction of secure NHSMail mechanism for distribution to non-nhs.net email recipients Indicate requirement for refresher training where logon not used for 6 months Note action to be taken when logon sharing is identified Reflect changes in CMC System data centre provider and locations, remove reference to SAS 70 standard Correct this document's publication location: CMC website rather than RMH intranet Refer to CMC Mobile Device Policy re Safari Update text re Business Continuity to reflect current situation	Mandy Shaw	

1. Summary

The development, implementation and management of a System Level Security Policy (SLSP) help to demonstrate understanding of information governance risks and commitment to address the security and confidentiality needs of a particular system.

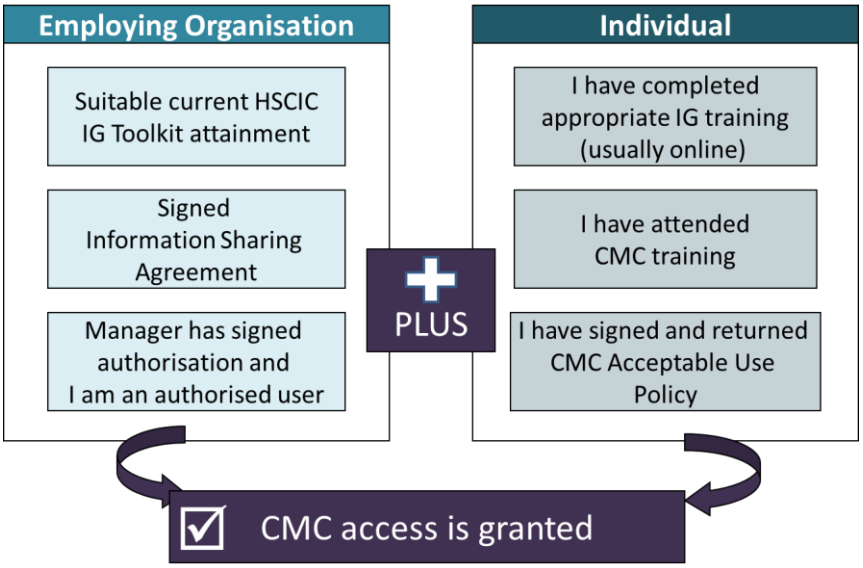
An effective SLSP will, therefore, contain a considered and specific view of the range of security policy and management issues relevant to a system and that may encompass a range of technical, operational and procedural security topics.

This SLSP relates to the Coordinate My Care (CMC) System, using the Liquidlogic **PRO**TOCOL platform hosted at System C.

This SLSP should be read in conjunction with the current version of the CMC System Information Sharing Agreement.

2. Contents

3. System Roles and Responsibilities



All CMC user organisations must formally agree to the CMC Information Sharing Agreement, and all CMC users must formally agree to the CMC Acceptable Use Policy.

All CMC user organisations using the CMC System from mobile devices must formally accept the CMC Mobile Device Operational and Support Policy.

All CMC user organisations are responsible for ensuring user access is up-to-date, that users comply with Information Governance standards, and that, in cases where these requirements are not followed, the incident is reported in line with the Information Sharing Agreement (ISA) procedure.

All CMC users are responsible for attending CMC training and, where not already done, completing appropriate IG training, and for complying with the CMC Acceptable Use Policy in addition to all relevant general Information Governance (Toolkit) requirements.

Organisations without IG Toolkit coverage can use the CMC Specific IG Toolkit (available on request) to ensure that all appropriate IG requirements are met. This Toolkit, a cut down and annotated version of the HSCIC Commercial Third Party toolkit, is aimed at assisting organisations such as privately owned nursing homes in achieving appropriate IG Toolkit coverage, attainment levels, and self-assessment.

Liquidlogic/System C are responsible for ensuring that system security is maintained as specified in this SLSP and that their staff access CMC data only in line with the Caldicott Principles, and only for support purposes.

4. System Management

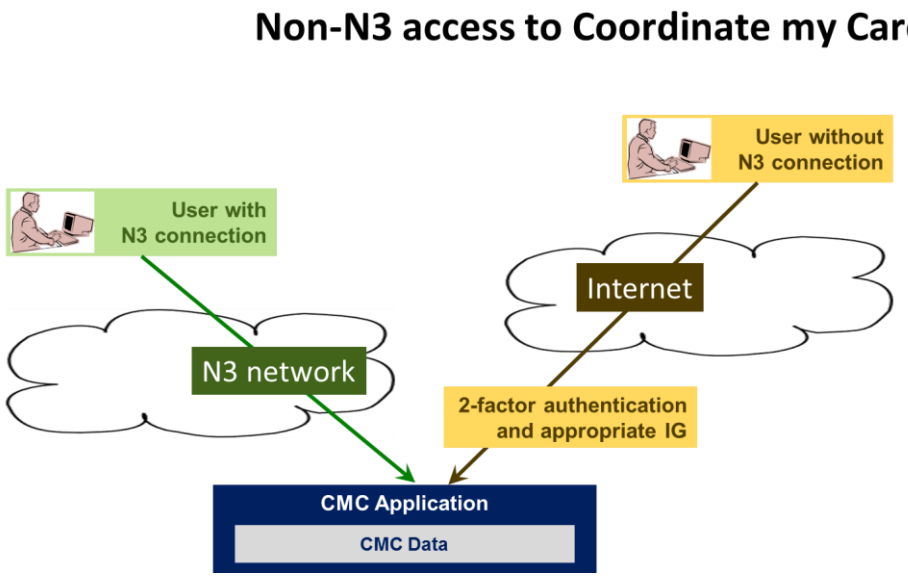
The CMC System comprises a dedicated instance of the Liquidlogic **PRO**TOCOL platform, configured to meet the requirements of Coordinate My Care. The CMC System is hosted and supported by System C and its subsidiary company Liquidlogic, the latter being responsible for development, configuration, deployment, and support of the system, the former for hosting.

The CMC System will be shared and used by NHS and non-NHS organisations for the purposes of accessing and recording care-related information.

There is a dedicated Data Warehouse, hosted at RMH. This has a secure feed from the CMC System. Patient identifiable data in the Data Warehouse will be used only for audit/compliance and Data Quality reporting aimed at improvements to, and governance of, the CMC system and its data. Management information reports, whether for distribution within the Royal Marsden or to a wider CMC community audience, will contain no patient identifiable data. Research activities will have no access to patient identifiable data. Any patient identifiable data extract from the Data Warehouse for use outside the CMC Team will receive specific signoff, and details of all such extracts will be made available to CMC Information Sharing Agreement signatories on application.

User access to the CMC System will typically be over the N3 network.

Non-N3 access is also available, controlled by 2-factor authentication using device-specific SSL client certificates managed through the Royal Marsden's cloud-based **Authen2cate** service.



The Authen2cate service is hosted in Amsterdam and Dublin. Traffic between CMC users and Authen2cate relates to browser client certificate management only. The CMC application at System C can be accessed over non-N3 only if a valid Authen2cate certificate is in place in the browser. To obtain this certificate, Authen2cate is responsible for registration challenge, certificate generation, and download. Once the certificate is present in the browser, connectivity becomes available to the CMC System; all application traffic travels direct between the user device and System C. No CMC System data will flow via Authen2cate. Data stored at Authen2cate is limited to non-N3 user registration details.

Initially all user access to the CMC System will be from a web browser. Please note that the use of a web browser from a mobile device will only be permitted providing the organisation has signed the CMC Mobile Device Operational and Support Policy.

Any necessary remote access to the system will be obtained either via the non-N3 Authen2cate two-factor authentication service as above or via the N3 remote access services and devices relevant to, and authorised by, the user's parent organisation. For example, mobile device access over N3 for out-of-hours GPs will be provided, controlled, secured, governed, and supported by the relevant OOH provider.

There are also RMH-imposed technical prerequisites for mobile device access to the CMC System – see the Mobile Device Operational and Support Policy, in particular re the use of Internet Explorer and of Safari.

In no situation may any CMC data (patient identifiable or otherwise) be downloaded or exported to the user's PC or device. An active network connection is always required to access CMC System data or functionality. Each organisation as a Data Controller in their own right will take responsibility for their users and ensure no CMC data is downloaded or stored on mobile devices. The only exceptions to this rule relate to CMC Team members responsible for reporting and/or who are on call in a Business Continuity situation however, in such cases, all mobile devices will be encrypted, and the relevant data will be removed immediately from the device when no longer needed.

Over time, automated interfaces will be made available from the CMC System, with access being controlled from the CMC System at the individual organisation level under appropriate governance. This interoperability will be available over the N3 network only. The only currently available such interfaces are:

- PDS integration via the PROTOCOL user interface (available to NHS smartcard users only);

- the CMC Automated Flagging service, whose information security and information governance aspects are documented in the Automated Flagging How-To Guide, available on request.

5. System Design

The CMC System comprises the following aspects:

- CMC System database servers, application servers, and integration servers, residing in a virtualised server and storage environment at System C's Northern Data Centre, and with appropriate network security protecting these servers and the links to, from, and between them;

- Completely separate environments as follows:

    - Live operational environment (99.90% availability Service Level Agreement), available via N3 (with or without NHS smartcard), or without N3 via Authen2cate;

    - User Acceptance Testing (UAT) environment, available via N3 or without N3 via Authen2cate;

    - Data UAT environment, used in the testing of migration data feeds and of automated flagging, available via N3 only;

    - Training environment accessible over non-N3 connections only;

- Replication of Live CMC data to System C's Southern Data Centre (this data transmission is unencrypted, but is held entirely within System C's internal network);

- Disaster Recovery provision via System C's standard DR offering, including availability of the entire Live CMC System at System C's Southern Data Centre;

- Regular transmission of data to the RMH-hosted dedicated CMC Data Warehouse over a dedicated SFTP connection via the N3 network;

- Backup of all CMC data every 24 hours in accordance with System C's backup strategy, using enterprise tools coupled with an automated schedule. All backups are non-invasive from a user perspective and normal system operations can continue while backups are running. Backup data is held locally on disk for speed of recovery from minor failures, as well as at offsite storage on tape. Note that as data is replicated continuously to the Southern Data Centre with a 3 minute delay, the use of backups for recovery (whether disk or tape) is regarded as an exceptional situation.

- **Note** that data on disk is not encrypted but is protected via the application level access controls in place. Data on removable media (tape backups) is, however, fully encrypted.

- **Note** that the current contract between RMH and Liquidlogic/System C explicitly ensures the delivery of the CMC application to 300 simultaneously active users at a defined level of application performance. User numbers and performance metrics are monitored by Liquidlogic/System C for capacity planning purposes. The **PRO**TOCOL platform supports considerably higher user numbers for other Liquidlogic/System C clients.

6. System Security

Security of the system shall be governed by this SLSP. Any necessary departure from this principle should be documented in this SLSP and accepted as a risk within CMC.

Access to the CMC System/data will be restricted to named staff. This must be via an individual user id and password logon, with the single exception of Urgent Care service view-only generic user ids as described in the next paragraph. (NHS smartcard access to CMC is supported, but only with an underlying CMC user id and password for each user.)

Urgent Care services may be issued with view-only generic user ids only once the requirement has been approved, and an audit trail mechanism suitable for clinical incident investigation has been formally agreed, by the Royal Marsden IG Lead.

Should CMC detect that any other logon has been shared, that logon will be disabled until documentary evidence is received that the individuals concerned have re-attended their annual Information Governance Training. A second occurrence will additionally result in the organisation's (for a GP practice, the CCG's) Caldicott Guardian being informed.

The issue and revocation of user ids and passwords, and provision/maintenance of access to each user at an appropriate level, will be controlled and processed directly by the Coordinate My Care Team.

CMC user enrolment is controlled as follows:

1) The user completes appropriate IG training where not already done, attends formal CMC training (full users) or studies CMC's tutorial video (read-only users), formally agrees the CMC Acceptable Use Policy, and is then enrolled in CMC with an individual user id and with a generic password, set to expire on first logon.

2) The necessary logon information (specific user id/generic password/CMC URL) is emailed to the user via NHSMail (taking advantage, where relevant, of the mechanism introduced by NHSMail in 2015 for secure distribution to non-NHSMail recipients).

3) (removed)

4) (removed)

5) The CMC Acceptable Use Policy and CMC Information Sharing Agreement demand that the CMC team are notified of leavers in a timely manner, and that the CMC team should, every two months, remind CMC user organisations of this requirement.

If password reset is requested for a logon that has not been used for 6 months or more, refresher training is mandated.

For non-N3 access, in addition to the above, CMC two-factor authentication requires each relevant user to be individually authorised to the Authen2cate service. An attempt to access CMC on a device/browser for which that user does not have a currently valid Authen2cate certificate will result in a challenge for a 4 digit registration code. The user can choose whether this code is sent, there and then, to their email or to their mobile 'phone (SMS). The email address or mobile 'phone number used will be as previously stored on the user's Authen2cate account by CMC. Successful entry of the registration code will permit download of a valid client certificate, as required for non-N3 use of the CMC application. Downloaded Authen2cate client certificates will automatically expire after 2 months, and can also be invalidated centrally by CMC.

Password validation rules are fully configurable by the CMC team. Currently, default expiry is 28 days, minimum length is 9 characters, and at least one of each of the following character types is mandated: lowercase, upper case, numbers, and special characters.

The system also asks the user to enter a security question to further verify who they are.

A signed, formal 3rd party confidentiality agreement meeting RMH policy exists between RMH and Liquidlogic/System C.

The CMC Acceptable Use Policy (formally agreed by CMC users) and CMC Information Sharing Agreement (formally agreed by CMC user organisations) together ensure that all staff (permanent, temporary and contractors) are:

- aware of the information security policies applicable in their work areas, aware of their personal responsibilities for information security, and aware of how to access advice on information security;
- appropriately trained in information governance and the safe use of the system;
- aware of any risks to information security within the system;
- formally authorised by the CMC Team to use the system.

The System shall incorporate the following security countermeasures:

- All CMC System network, server, and storage components are housed in secure areas under the control of System C, who also take responsibility for appropriate, timely operating system and middleware updates and for appropriate, up-to-date anti-virus, anti-malware, and anti-intrusion measures;
- All non-N3 client certificate management components are housed in secure areas under the control of Authen2cate, who also take responsibility for appropriate, timely operating system and middleware updates and for appropriate, up-to-date anti-virus, anti-malware, and anti-intrusion measures;
- Appropriate server-side security measures are in place in the application to prevent browser caching of sensitive data;
- The CMC application has a configurable inactivity timeout, currently set to 30 minutes, with a warning shown to the user 2 minutes earlier. When the timeout expires, the user cannot operate the CMC application without logging in again; when they do so, they are returned to where they left off. **Note** that because the timeout login prompt does not at present conceal the last viewed data, this functionality should be used in conjunction with a standard Windows screen lock timeout;
- Only authorised staff of Liquidlogic and System C are able to access the system for support purposes, with access mechanisms and access privileges made available as appropriate in order for them to be able to conduct the appropriate level of support and maintenance.

System C/Liquidlogic have the following controls in place:

- ISO9001, ISO27001 compliance;
- Data Centres segregated from System C corporate network, with access to DCs limited at the network domain level (i.e. using DNS policies) to specified users;
- HSCIC IG Toolkit (IGSoC) compliance for N3 connectivity;
- Application-level (PROTOCOL) user access controls, restrictions, and auditing apply to Liquidlogic and System C staff just as they do to other CMC users;
- If any PI data is inadvertently included in a JIRA (support call), this is immediately deleted by policy and the originator informed;
- Training/onboarding for all System C staff includes mandatory Data Protection training;
- All staff with physical or network access to the Data Centres undergo regular CRB checks (this includes, for example, the Business Intelligence team and the team responsible for development and testing of application integration functionality).
- Relevant network security measures in place include firewalls, network segregation and penetration testing. System C have a rolling penetration test programme covering all **PRO**TOCOL customers hosted in their data centre, including CMC, but are not able to share any further details. There will be additional penetration testing scheduled specific to non-N3 access to CMC;
- Access will be restricted to only users who have a legitimate business purpose for accessing the system. The database can only be accessed for purposes which directly contribute to the diagnosis, care and treatment of an individual and/or the audit/assurance of the quality of healthcare provided. Secondary use does not contribute to the diagnosis, care and treatment of an individual or to the audit/assurance of the quality of healthcare provided and as such access to and use of personal information held in the CMC System must be avoided unless explicit written consent from the patient is obtained or otherwise covered in law, such as where a valid section 251 application to set aside the common law duty of confidentiality has been obtained by the National Information Governance Board. The only exception to this rule is where staff are a member of a New Safe Haven (e.g. Informatics) and appropriate approval has been granted within the Trust;
- Staff should only have access to the data that is necessary for the completion of the business activity which they are involved in. This is reflected in Caldicott 6 Principles; access should be on a strict need-to-know basis;
- This Policy and project supports Information Governance Toolkit requirements, particularly those which state that the confidentiality of service user information must be protected through use of pseudonymisation and anonymisation techniques where appropriate.

7. Operational Processes

The patient identifiable/sensitive data will be captured in the following ways:

- entered by CMC System users (the vast majority of the data);

- entered by specifically authorised CMC users from faxes or securely emailed scans sent by user organisations (supported only where the sending user organisation is temporarily unable to access the CMC System direct, and where the information exchange mechanism in use is IG Toolkit compliant);

- migrated from the previous Adastra-based CMC System (whether manually by users in the relevant organisation, or via an automated and securely transmitted data feed).

The downloading of any data from the system to any device, other than by the CMC Team for the purposes of reporting or business continuity, is prohibited without the express permission of the Royal Marsden Caldicott Guardian; printing or screenshots of any data from the system are prohibited, with the following two exceptions:

- Copies of individual patients' CMC records, which are printed (as standard procedure) for the patient to keep;
- Printed or stored copies of CMC operational reports (e.g. Patient List Report) for use in meetings where no CMC System connectivity is available; the printed or stored copy must be destroyed securely immediately after the meeting.

All desktop computers, laptops, and mobile devices on which the CMC System is used must be able to be formally wiped of all data on the local hard disks to an approved standard. In the case of laptops and mobile devices, this must be able to be done remotely.

When the system or its data has completed its purpose/has become redundant or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data:

- The servers for this system are all virtualised. When the purpose of this system has been completed all virtualised copies of the system will be formally deleted.

8. System Protection

The System shall benefit from the following resilience/contingency/disaster recovery arrangements:

- The servers comprising this system are all virtualised. As such there are benefits in the flexibility and speed with which the system can be reconfigured / relocated etc in the event of a major disaster or other emergency;

- The system is hosted at System C's Northern Data Centre. In the event of an emergency it will be possible to make use of the automatically replicated copy of the CMC System at System C's Southern Data Centre.

In the event of serious disruption or total system failure, RMH shall ensure business continuity by the following means:

- The decision can be taken, if appropriate, to invoke System C's DR provision for the CMC system;

- For interim cover (or for brief planned downtime) the on call CMC clinician can provide CMC System users with appropriate information on request via the CMC Data Warehouse's 'All Data' reporting facility, which will reflect CMC care plan content at the end of the previous day.

In the event of a security or confidentiality breach occurring, the incident reporting procedure detailed in the Information Sharing Agreement shall be followed.

9. System Audit

The System benefits from the following audit arrangements and capabilities:

- The system maintains a structured audit trail of all create/update/delete/view activity relating to any aspect of a patient care plan;

- The CMC team can supply regular or on-demand audit reports as input to CMC user organisations' confidentiality audit activities;

- The CMC team can carry out detailed audit trail analysis for incident investigation;

- A bimonthly listing is distributed to each CMC user organisation (i.e. to each Data Controller) showing users authorised to access the system and their associated security levels.

10. Risk Assessment

The System shall be risk assessed by the system's Royal Marsden Information Asset Administrator, at Senior Management level, every quarter by applying an appropriate method. All risks shall be scored using the Department of Health Risk rating formula.

A risk management/security improvement plan shall be established and managed by the System's Royal Marsden Information Asset Administrator, in order to address all relevant risks.

11. System Level Security Policy Ownership

This SLSP shall be the responsibility of the Royal Marsden Information Asset Administrator, at Director level. It will be reviewed on an annual basis for its completeness and for relevant update.

The SLSP shall be available/distributed on the Coordinate My Care website.

12. Data Protection Legislation

The Data Protection Act 1988 requires all Data Controllers which are processing personal data to notify the Information Commissioner's Office. The Royal Marsden NHS Foundation Trust has a valid entry on the Data Protection Register (registration number. Z5146911). This entry covers the personal data that is held on the CMC System and how it is used.

Appendix 1: Equality Impact Assessment

Screening form

Policy/ service: System Level Security Policy for the Coordinate My Care System

Leads: Dr Julia Riley **Department:** Coordinate My Care

Please provide details of all people involved.

New or existing policy or activity: New Policy **Policy Number**:

Aims and outcomes	Description/Details
Give a brief summary of the policy aims, purpose, objectives and outcomes (include any aims in relation to equality and diversity)	System Level Security Policy for the Coordinate My Care System to ensure security of data and address information governance risks.

Questions for you to use in the Screening Process	Yes	No
1. Will or does the policy affect our patients or the public directly or indirectly or our workforce or our employment practice?	X	
2. Could the policy involve or have an impact upon the Equality Duties to:		
• eliminate unlawful discrimination		X
• promote equality of opportunity		X
• promote good relations between diverse groups		X
3. Will or does the policy have an actual or potential for a differential impact on patients, staff or other people because of:		
• **Race** (race, colour and nationality (including citizenship), ethnic or national origins)		X
• **Disabled people** (including mental, physical, sensory, long term health, learning disabilities)		X
• **Gender** (male, female, transgender)		X
• **Age** (young and old)		X
• **Religion or belief** (inc non-believers)		X
• **Sexual orientation** (lesbian, gay, bisexual)		X
• **Gender reassignment** (the process of transitioning from one gender to another)		X
• **Pregnancy/maternity**		X
• **Marital/ Civil Partnership status**		X

4. What evidence or data have you used to screen the policy or service? List below, giving details including any explanation or actions taken to address impact. **Policy has no differential effect on any group.**	
Assessment of Screening **Assessing policy/ activity relevance to equality and diversity**	**Scoring of relevance to equality** **Questions 2 and 3 have high relevance to equality** Based on the responses above, does the policy or activity have ***high relevance*** to equality and require a full Equality Impact Assessment: **NO** If **NO**, the process stops here. sign below and return to Lisa Neden, Diversity Manager, HR, Sutton Sign: If **YES**, a full EIA is required using the EIA template in **Stage 2**. Please contact Lisa Neden for advice on completing the EIA if required.