Overview of the CMC Information Governance Pathway

Version Control

Version Number	Amendments made	Changes made by	Date
2	Add footer Add 'Information Governance Roles in Brief' section	Coordinate My Care IT Architect	26th February 2015
2.5	Update to reflect CMC e-Learning provision	Coordinate My Care IT Architect	21st October 2015
2.6	Remove reference to obsolete Out of Hours S.O.P. Mention New User Form as alternative to User Access Form Update diagram	Coordinate My Care IT Architect	2nd November 2015
2.7	Rules concerning CMC IG document reproduction and linking Update text and diagram to reflect training self-certification	CMC IT Architect	17th May 2016
2.8	Updating the Figure 1 to reflect HSCIC name change to NHS Digital and retirement of the New User Form. Update the website address to link to IG resources. Clarifies that the AUP is on screen only. Removal of face to face training option. Designating 'self-certification' of competence without training as Waiver of Training. Clarity that publishing the care plan in the first instance implies legitimate relationship with the patient.	CMC Quality Clinical Manager	04th April 2017
2.9	Updating the Figure 1 to reflect new name for the toolkit from NHS Digital. Removal of the paragraph on the CMC specific mini IG Toolkit, its use by nursing homes and annual accreditation due to the more nursing home sensitive NHS Digital Data Protection & Security Toolkit which is now in use.	Interim Director of Nursing	14/06/2018

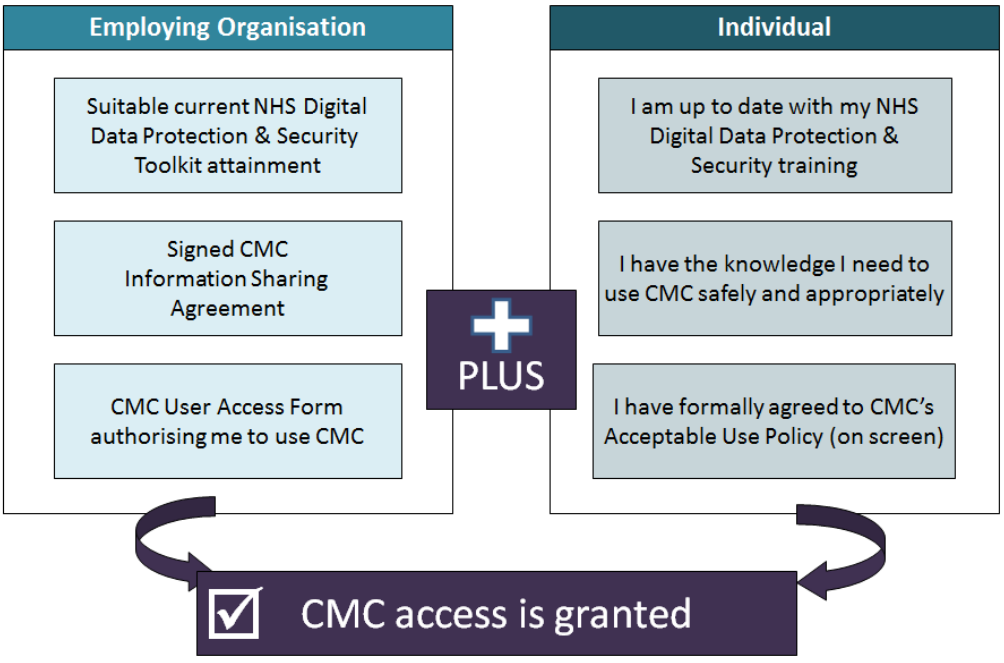

Fig 1. Summary of CMC IG requirements for CMC access

CMC IG for Individual Users

Each CMC user must be listed on a CMC User Access Form signed by his/her manager; must register for and complete appropriate online CMC training ('e-Learning'), receive face to face cascade training where available or self-certify sufficient knowledge to permit safe and appropriate use of CMC and of the information it shares (Waiver of Training form); and must be up to date on his/her NHS Information Governance (IG) Training.

Users must also formally agree to the CMC Acceptable Use Policy (which will appear on screen when logging in for the first time, which explains the purpose and context of CMC, the responsibilities of the user, and the information governance and other requirements with which they must comply.

Each CMC user organisation agrees, via the CMC Information Sharing Agreement (see next section), to share its entered CMC information with all such organisations, which means that all individual users agree to share any CMC information they may enter onto the CMC System.

CMC IG for the Organisation

CMC has a single Information Sharing Agreement across all user organisations, because it uses the principle of joint Data Controllers (each CMC user organisation is the Data Controller for the CMC records it creates). The user organisation must sign this ISA, must complete the User Access Form listing all authorised users, and must comply with an appropriate IG Toolkit.

CMC IG: the Patient Perspective

Before a record can be stored on CMC, the patient must consent to the use of their data by professionals in the course of their care; by the CMC team in ensuring clinical quality; and, where not patient identifiable, for appropriate research. This consent model is documented in CMC's Patient Information Leaflet.

Although the patient (and indeed the originating clinician) has consented to have the CMC record shared, they both need to know that the system will log who has looked at it, and what information they might have edited or updated.

CMC logs all access to the record, whether or not any changes are made. Should an incident be raised regarding access to a patient's record, a detailed auditable log can be produced to show exactly who accessed the record and what edits were made at any one time. There is the added value that CMC can identify which professional was responsible for any clinical decision made for the patient at any particular time.

In addition, no person can access the record unless they have an explicit, self-claimed, auditable legitimate relationship with the patient. Publishing the care in the first place implies this legitimate relationship exists.

Mobile Device Usage

Any organisation wishing to use CMC on mobile devices must formally agree to the CMC Mobile Device Operational and Support Policy.

CMC and non-NHS organisations without an N3 or Health & Social Care Network connection.

Because Coordinate My Care is a centrally hosted system accessed only via the web browser, the IG requirements placed on non-NHS organisations (e.g. Nursing Home) accessing Coordinate My Care via the non-N3 two-factor authentication route (Authen2cate) are limited. Specifically, such organisations do not need coverage of any IG requirements that relate to the hosting of IT systems or data.

CMC IG Documentation

CMC's IG documents are the latest published versions of:

- CMC Information Sharing Agreement (see above)
- CMC Participating Organisations List (available on request)
- User Access Form (see above)

- Acceptable Use Policy (on screen – see above)
- Waiver of Training (see above)
- Patient Information Leaflet (see above)
- Mobile Device Operational and Support Policy (see above)
- System Level Security Policy, covering the information security of the CMC System
- Privacy Impact Assessment, including a detailed Data Protection Act 1998 compliance checklist
- Business Continuity Plan
- CMC Automated Flagging How-To Guide, covering the IG aspects of CMC's automated urgent care flagging service

Reproduction and Linking

Please note that CMC's IG documents may only be reproduced whole, in their original format, and after checking with CMC that you have the most recent version. Linking to the relevant document on the CMC website (see http://coordinatemycare.co.uk/healthcare-professionals/getting-started-information-governance/) is always the preferred method.

Base Legislation

The legislation on which CMC's IG Pathway is based is listed in Appendix A of the Information Sharing Agreement.

Information Governance Roles in Brief

Caldicott Guardian: a care professional with specific responsibilities to drive and ensure the application of the Caldicott Principles within their organisation.

Senior Information Risk Owner: a named board-level individual with responsibility for IG risk management within their organisation.

Information Asset Owner: a named senior individual who takes responsibility for understanding the information held; how information is moved; and who has access and why.

Information Governance Lead: a named individual who takes responsibility for co-ordinating, publicising and monitoring standards of information handling within the organisation and for developing and implementing an IG improvement plan. The IG Lead also ensures that Data Protection & Security Toolkit assessments are submitted as required.