Coordinate My Care
Mobile Device Support and Operational Policy

Purpose of Document

This document describes the specific technical, security hardening, and support responsibilities of CMC user organisations wishing to use the CMC System from mobile devices.

Formal agreement to this document is required before any organisation may make use of CMC from a mobile device.

Mandy Shaw, IT Architect, Coordinate My Care
Version 2.0, 12th July 2016

Version Control

Version Number	Amendments made	Changes made by	Date
1.1	Add signoff section	Coordinate My Care IT Architect	7th May 2014
1.2	Situation clarified re use of Safari on Apple devices with non-N3 connections to CMC Text reviewed, minor typo fixed	Coordinate My Care IT Architect	24th March 2015
2.0	Amendments to reflect new Intersystems system, and potential for usage with BYOD devices	Coordinate My Care IT Architect	12th July 2016

Table of Contents

1. Responsibilities

The following responsibilities apply to CMC users and user organisations in relation to the use of CMC on mobile devices:

- CMC users and user organisations must accept that CMC data will be available to a mobile device only when that device is experiencing adequate data signal;
- CMC users and user organisations must accept the limitations inherent in using the CMC application on a smaller form factor device;
- CMC users and user organisations must in particular accept that certain CMC information displays and application functionality will be reduced in scope or unavailable from a mobile device, e.g. patient address absent from patient banner, EMIS Web in-context link not available, printing functionality absent (a detailed list of these differences is available on request);
- CMC users and user organisations must accept that a limited list (available on request) of mobile devices/browsers will be formally supported by CMC at any given time, while other mobile devices/browsers will be supported on a best efforts basis only (under some circumstances using the standard CMC desktop application);
- Users, when logging on, may select only the organisation that owns the device, except where the selected organisation's agreed Bring Your Own Device (BYOD) policy is being used;
- The CMC user organisation must take full responsibility for all but BYOD devices in terms of (but not limited to) build, maintenance, replacement and support; they must also take full responsibility for the definition and implementation of all BYOD policies;
- All users of the mobile devices, when logged on to CMC, are bound as usual by their currently selected CMC user organisation's information governance, information security and mobile device usage policies;
- Access to CMC data on a mobile device imposes specific requirements in relation to browser software and security hardening (see section 2 below).

In particular, the CMC user organisation will supply:

- Build/commissioning of the devices;
- Compliance of the devices to CMC browser and security hardening requirements (see section 2 below);
- The IT infrastructure (data connectivity, any N3 access, all necessary user training and reference material) for the mobile devices to connect to and access the CMC system;
- User support for any issues experienced with the devices or with N3 connectivity (whether out-of-hours or not).

Coordinate My Care will not:

- Be held responsible for locking down/restricting access to other sites/applications on the devices;
- Be held responsible for any patient identifiable data found on a device;
- Be held responsible for loss of or damage to the devices, or for maintenance required for the devices;
- Be held responsible for failures to access the CMC application caused by permanent or temporary lack of adequate data connectivity or by failure of a user organisation's N3 access infrastructure;
- Provide end user support for device specific or connectivity related issues;
- Provide funds to cover the cost of devices, connectivity, insurance or warranty.

Coordinate My Care support provision:

- Telephone support is provided by CMC to the user organisation and to users re CMC application/process issues only (*not* re device, data, or N3 connectivity issues), and within office hours only (Monday to Friday, 9am-5pm, excluding Bank Holidays), except for password resets or CMC application down (Severity 1) issues.

2. Device Requirements and Security Hardening

The specific requirements of mobile device access to the CMC application are, additionally:

- The CMC user organisation's IG Toolkit coverage must apply to all mobile device environments used for CMC access;
- A policy must be in place that explicitly prevents patient identifiable data held within the CMC application from being saved onto, or transmitted from, the device in any way, whether encrypted or not;
- The device should be configured in such a way as to prevent screenshots from being taken; if this is not possible for technical, operational, or BYOD reasons, a policy must be in place that explicitly prevents screenshots being taken from within the CMC application.;
- Wherever possible the device must be configured to be able to be wiped remotely by the owning organisation in the case of loss or theft. CMC would also encourage user organisations with BYOD policies to include advice and guidance in these policies concerning the deployment of remote wipe functionality.

3. Notes on Non-N3 Usage of Mobile Devices

Non-N3 access to CMC uses the Authen2cate two-factor authentication service (please see the CMC System Level Security Policy for more information).

Specific Authen2cate requirements for Apple devices (Mac, iPad, iPhone) are as follows:

1. Users will need to enter a password for the certificate during their registration/download;
2. On Apple mobile devices, users will have to use Safari, as it is the only browser iOS will allow to read the keystore.

4. Signoff

Mobile Device Operational and Support Policy Coordinate My Care

The parties to the agreement are as follows;

Organisation **Address** **Contact Details**	The Royal Marsden NHS Foundation Trust 203 Fulham Road, London SW3 6JJ
Signature	
Name:	Dr Nicholas van As
Designation:	Medical Director & Caldicott Guardian
Date:	22/02/17

Organisation **Address** **Contact Details**	
Signature	
Name:	
Designation:	
Date:	