{{!orglarge **}}**

Regional Health and Social Care Information Sharing Agreement

Data Flow – PC200012 – Connected Care EMIS XA Proof of Concept:

Schedule K – Processing and Sharing Specification (signature required)

Schedule L – Initial Data Protection Impact Assessment

Visit www.regisa.uk for the narrative and the latest versions of Schedules

Schedule K – PC200012 – Connected Care EMIS XA Proof of Concept

Sharing Requirement Identifier:	PC200012
Sharing Requirement Name:	Connected Care EMIS XA Proof of Concept
Sharing Requirement Start Date:	01 June 2021
Sharing Requirement End Date:	30 June 2022
Sharing Organisation:	{{!org_es_:font(name=calibri,size=10) }}
Direct Care or Other Uses:	Direct care
Risk Sharing and Indemnity:	A promisee organisation
Sharing Data Controllership:	Joint control with Frimley Health NHS Foundation Trust as lead controller
Data Processor(s):	EMIS - SoftCat - Graphnet - System C - Microsoft
Status:	Final
Version:	v1.1

Summary of the Sharing Requirement Purpose

The purpose of the Connected Care Interoperability solution is to enable information about an individual's medical condition and social care packages and requirements to be shared electronically across subscribing health and social care organisations in order to ensure that the care provided is safe and consistent with patients' existing risks, diagnoses, conditions, problems, medication and other treatment. These records are known locally as Connected Care.

The purpose of this joint processing and sharing specification is to support a proof of concept that is confirming the ability of the EMIS XA solution to improve the flexibility and timeliness of the current overnight extracts and data flows from EMISweb into the Connected Care solution.

The primary objectives of the EMIS XA proof of concept are, using a small number of volunteer practices:

1. To confirm that the enhanced detail available through EMIS XA is usable through Connected Care and of significant additional clinical value;
2. To demonstrate that practices (as the source data controllers) have adequate control over EMIS XA based data flows;
3. To show that using EMIS XA does not have a negative impact on EMISweb performance for the practices themselves;
4. To verify that messages from Connected Care will be handled appropriately by practices' EMISweb workflow solutions;
5. To ensure that using EMIS XA does not degrade the timing and availability of GP data within Connected Care; and
6. To prove that the enhanced EMIS XA data feeds can replace the current, restrictive overnight data feeds from EMIS into Connected Care.

Legal Basis for the Processing

Unless a patient has opted out from sharing and the sharing organisation has accepted the patient's opt-out the legal basis for sharing and viewing the shared records includes provisions of Section 251B of the Health and Social Care Act 2012 (as amended by the Health and Social Care (Safety and Quality) Act 2015):

2. The sharing organisation must ensure that the information is disclosed to:
   (a) persons working for the sharing organisation
   (b) any other relevant health or adult social care commissioner or provider with whom the sharing organisation communicates about the individual; and
3. So far as the sharing organisation considers that the disclosure is:
   (a) likely to facilitate the provision to the individual of health services or adult social care in England
   (b) in the individual's best interests.

Unless a patient has opted out from sharing and the sharing organisation has accepted the patient's opt-out the legal basis for viewing the shared records is also provided by General Data Protection Regulation:

1. 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"; and
2. 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".

Where access to confidential data is legitimate, the common law duties of confidentiality are satisfied because consent to view a patient's record is implied where the patient concerned agrees to be referred to a service or where the patient concerned refers themselves or presents to a service.

With respect to this requirement a core purpose of the data usage in this instance is to validate the data processing arrangements and therefore the legal basis for the requirement also includes General Data Protection Regulation:

1. Article 5(1)d
   "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

Summary of the Sharing Requirement Process

The technical platform for Connected Care is the CareCentric product from Graphnet Limited. CareCentric is a HSCN/N3 web based secure system that allows secure cross boundary access to patient information held in the shared records.

For the purposes of this schedule the sharing process is as follows:

1. The Connected Care data is extracted from practices' clinical systems via EMIS XA;
2. The Connected Care extract process normally runs every 24 hours. However, as part of the proof of concept extracts will also be run on an ad-hoc basis;
3. The extracted data is securely transmitted to the Graphnet CareCentric data repository by means of tried and proven EMIS XA data extraction technologies;
4. The Connected Care data is stored in the CareCentric data repository housed in the fully accredited and secure Microsoft Azure data centre;
5. The Connected Care data is made available to and accessed by health and social care practitioners with a legitimate relationship with the individual, using the CareCentric system and within the constraints set by the Connected Care opt-in/opt-out and consent model;
6. Subject to a legitimate relationship being established the data is made available through the CareCentric system for viewing by the users in the user organisations identified in this Schedule and in accordance with the User Service Profiles identified in this Schedule; and
7. For the proof of concept where appropriate, the data types received from provider systems as set out from point 42 onwards of the section "Shared Categories of Data" below are transferred from Connected Care via EMIS XA into the patient's registered practice workflow system. These data transfers to the practice clinical system via EMIS XA will occur as soon as the data is received by Connected Care.

It is the EMIS XA Explorer tool that enables more timely access to the richer EMISweb data held in the EMIS X "data lake" and that provides appropriate return workflows for selected patient risk and status into practices' EMISweb systems.

Summary of the Sharing Requirement Privacy Arrangements

The privacy arrangements are considered satisfactory as:

1. Access to view data is managed in accordance with the RBAC (Role Based Access Control) arrangements for Connected Care;
2. The data is accessed in accordance with the opt-in/opt-out and consent model as summarised by points 3 to 5 below;
3. No data is made available for sharing where a patient has indicated to the patient's practice that the patient does not want their data to be shared and where the practice has recorded this election within the patient's record;
4. Where any of the data controller organisations other than the patient's practice are notified by the patient that the patient does not wish to have the patient's data shared the data controller organisation directs the patient to the patient's practice for the purposes of making this election;
5. Explicit consent to view the shared data relating to an individual who has not opted out is not required for the purpose of provision of care to the patient;
6. Data items are not made available for sharing where a practice has indicated that the data items concerned are not to be shared;
7. Only the data as summarised in Shared Categories of Data below is extracted from the practice clinical systems;
8. As with the standard GP data extracts to Connected Care, sensitive diagnoses are excluded from General Practice data;

9. Connected Care includes an audit trail showing which user accessed a data subject's records; and
10. Key security aspects include:
    a. the physical security of the system servers
    b. the use of secure internet protocols for all data transactions
    c. multi-factor authentication for user access to the system
    d. role based access profiles to control user permissions.

The Sharing Organisations (data providers and data controllers)

For the purposes of this sharing requirement the sharing organisations may determine the purpose and use of the personal confidential data including creating, editing, archiving and deleting the data.

The sharing organisations are all organisations of all classes that have:

1. Signed the Regional Health and Social Care Information Sharing Agreement; and
2. Signed a copy of this Schedule to the Regional Health and Social Care Information Sharing Agreement.

The User Organisations

The following classes of Regional Health and Social Care Information Sharing Agreement member organisations have committed to use the personal confidential data identified in this document at the point of care in a manner compliant with the Regional Health and Social Care Information Sharing Agreement and solely for the purposes defined in this document.

The user organisations include all practice organisations that have:

1. Have signed the Regional Health and Social Care Information Sharing Agreement; and
2. Is the patient's registered practice or are providing care on behalf of the patient's registered practice.

The other classes of user organisation are those organisations that have signed the Regional Health and Social Care Information Sharing Agreement and that are:

1. Independent sector health care providers (including primary care and GP alliances and networks);
2. Independent sector social care providers (adults and children);
3. Local authorities;
4. NHS Trusts, including:
    a. Acute service providers
    b. Community service providers
    c. Emergency services
    d. Mental health providers
    e. Specialist service providers; and
5. Voluntary sector providers (commissioned or coordinated by Local Authority and NHS organisations).

The User Access Model and Service Profiles

The level of detail and the categories of data that can be viewed are dependent on the sector in which the care and services are being provided and the service profile the user is allocated to. There are five user service profiles in the Connected Care role based access control (RBAC) model. These are:

1. Clinical Practitioner;
2. Health Professional;
3. Social Worker;
4. Admin/Clinical Support; and
5. Clerical.

Details of the interaction between the service profiles and the data segments are summarised within Annex D.1 Sharing Service Profiles.

The Shared Categories of Data

The following categories of data are shared as part of the Regional Health and Social Care Information Sharing Agreement using the Connected Care solution.

The normal categories of patient data shared from practice clinical systems are:

1. Person Details and Demographics;
2. Allergies;
3. Events;
4. Health Promotion;
5. Medications;
6. Preventative Procedures;
7. Problems;
8. Procedures;
9. Referrals Details;
10. Results; and
11. Social / Family History.

The additional categories of patient data shared from practice clinical systems for the purposes of the proof of concept are:

12. Care Plan data;
13. Clinical Frailty Scale data;
14. Nominated pharmacy details;
15. Appointment information;
16. Cause of death; and
17. Associated free text.

Data that is shared by the local authorities and the provider trusts for use alongside the abovementioned includes:

18. Person Details and Demographics;
19. Next of Kin;
20. Risks And Warnings;
21. Alerting;
22. Allergies;
23. Admissions;
24. Appointments Details;
25. Assessment;
26. Associated People;
27. Care Plan Interventions Details;
28. Care Plan Problems Details;
29. Care Plans Details;
30. Carer Details;
31. Children's;
32. Diagnosis Details;
33. Diagnostic Tests;
34. Discharges;
35. DOLs (Deprivation of Liberty);
36. Early Interventions;
37. Electronic Documents;
38. Referrals Details;
39. Risk Management plans;
40. Safeguarding; and
41. Service Planning.

The data types that may be shared with practices by the provider trusts using EMIS XA's workflow messaging include:

42. Admissions;
43. Care Plans Details;
44. COVID-19 Test Results;
45. Discharges;
46. Medication Changes;
47. Potential Diagnoses and Alerts; and
48. Transfers of Care.

Availability of these categories of data through Connected Care is to be phased in during the period of this sharing specification and not all of the data categories identified above are expected to be available through Connected Care immediately.

By design, the shared data excludes particularly sensitive records. The clinical terms and Read Codes that are used to identify these sensitive data records are presented in the attached Annex D.5 Excluded Read Codes.

Summary of the Data Protection Impact Assessment

The Connected Care project has been carefully designed to place the interests of patients uppermost. Concepts of informed consent and compliance with the Caldicott and Data Protection Principles have been incorporated into the software design.

This schedule supplements the data sharing currently authorised by controllers against the existing joint processing and sharing schedules PC160001, PC170007 and PC170011. The existing Data Protection Impact Assessments DPIA0001 (Clinical Platform) and DPIA0002 (Analytics Platform) also apply to this joint processing and sharing specification.

The design and data protection and security risks for Connected Care as a whole and the associated security measures and safeguards have previously been subjected to a detailed and rigorous impact assessment by representatives from each of the participating partner organisations acting together as the IG Steering Group that oversees Connected Care.

The information governance risks relating to the additional processing arrangements described in this schedule have also been reviewed by the IG Steering Group and the IG Steering Group is satisfied that all appropriate technical and physical measures against unauthorised or unlawful access, accidental loss or destruction of care data are in place for Connected Care as a whole and for the new processing arrangements.

The four key additional risks are set out in the Schedule L document.

Summary of Consultations

As the uses of the identifiable data covered by this sharing requirement are restricted to existing arrangements for the provision of care, no explicit and direct consultation has been carried with the public in respect of this sharing requirement.

Patient groups were established in east and west Berkshire for the specific purpose of commenting on the sharing planned and on the information governance put in place to protect the confidentiality of the data. These groups include CCG and Healthwatch patient representatives with other self-selecting volunteers to form groups that have current awareness with health and social care issues.

Agreement Implementation Status

On behalf of the Sharing Organisation I confirm that the information sharing arrangements described in this schedule are agreed and the information described in this schedule is to be made available to the User Organisations and individuals identified in this schedule starting on the Sharing Requirement Start Date and ending on the Sharing Requirement End Date.

Agreed by **{{!guardian_es_:font(name=calibri,size=10) }}**
as Caldicott Guardian / Designated Officer / Data Protection Officer / SIRO, for and
on behalf of {{!org_es_:font(name=calibri,size=10) }}
{{!addr_es_:font(name=calibri,size=10) }}.

End of Schedule K

Schedule L – PC200012 – Connected Care EMIS XA Proof of Concept

This schedule should be read in conjunction with the existing Connected Care Data Protection Impact Assessments DPIA0001 (Clinical Platform) and DPIA0002 (Analytics Platform).

Technology Risk

1. Does the proposed change apply new, innovative or additional information technologies that have substantial potential for privacy intrusion? **… Generally, no. The core EMISweb, EMIS XA and Connected Care technologies have been tried and proven over many years and access to the technology is controlled by strict role based access controls and security and audit measures. This method is more secure and safer than alternative methods such as printed records, fax and letter.**

Identity Risk

2. Does the proposed change involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes? **… No. While datasets will all be identifiable using NHS Number this policy is in regular use in health and social care. Furthermore, the technology and processes are tried and proven over many years.**
3. Does the proposed change have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions? **… No. The existing approach already requires identifiable data.**
4. Does the proposed change combine, compare or match data from multiple sources in a manner that can be used to identify data subjects? **… No.**
5. Does the proposed change include the processing of biometric or genetic data that can be used to identify data subjects? **… No.**
6. Does the proposed change result in the processing of data concerning vulnerable data subjects? **… Yes. However, the purpose of the processing includes improving the quality of care and safety of vulnerable data subjects.**
7. Does the proposed change result in the processing of personal data which could result in a risk of physical harm in the event of a security breach? **… No.**
8. Does the proposed change have the effect of systematically monitoring a publicly accessible place on a large scale? **… No.**

Automation and Profiling Risk

9. Does the proposed change include profiling on a large scale? **… No.**
10. Does the proposed change include evaluation or scoring? **… No.**
11. Does the proposed change include automated decision-making with significant effects? **… No.**
12. Does the proposed change include systematic and extensive profiling or automated decision-making to make significant decisions about people? **… No.**
13. Does the proposed change include processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them? **… No.**
14. Does the proposed change include profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit? **… No.**
15. Does the proposed change include processing involving preventing data subjects from exercising a right or using a service or contract? **… No.**

Organisational Risk

16. Does the proposed change involve multiple organisations that do not have a prior history of working together and sharing information? **… No. The partner organisations have an extensive history of sharing and using this data.**
17. Does the proposed change involve innovative organisational solutions? **… No. Organisational processes do not change with this solution.**
18. Does the proposed change involve multiple organisations that do not have a prior history of working together and sharing information? **… No. The organisations concerned have considerable history of working together in the provision of care.**

19. Does the proposed change involve data processor organisations that do not have a prior history of working with similar shared information? … **No. The chosen suppliers are long-standing suppliers in the field and have extensive experience with similar data.**
20. Are new processes and relationships required to manage issues with the technology solution and with the accuracy, consistency and completeness of the shared information? … **No. This is an extension of previous sharing arrangements and the core Connected Care technology is tried and proven.**

Data Risk

21. Does the proposed change include processing of special category data on a large scale? … **Yes. In respect to the batch-based processing of the data extracts.**
22. Does the proposed change combine, compare or match data from multiple sources? … **No.**
23. Does the proposed change include processing of personal data without providing a privacy notice directly to the individual? … **Yes.**
24. Does the proposed change include processing of personal data in a way which involves tracking individuals' online or offline location or behaviour? … **No.**
25. Does the proposed change include systematic processing of sensitive data or data of a highly personal nature? … **Yes. However, the purpose of the processing includes improving the quality of care and safety of vulnerable data subjects.**
26. Does the proposed change include processing on a large scale? … **Yes. In respect to the batch-based processing of the data extracts.**

Exemption and Exclusion Risk

27. Does the proposed change include processing of criminal offence data on a large scale? … **No.**
28. Does the proposed change relate to data processing which is in anyway exempt from legislative privacy protections? … **No.**
29. Does the proposed change's justification include significant contributions to public security measures? … **No.**
30. Does the proposed change involve systematic disclosure of identifying data to, or access by, third parties that are not subject to comparable privacy regulation? … **No.**

Summary of the Data Protection Impact Assessment

The answers to the above risk questions indicate that a DPIA: ***~~is required /~~ is not required*** (delete as appropriate).

Risks – identified and assessed (prior to mitigation and controls)

The table below sets out the new risks presented by the solution as well as the main areas of risk for the Connected Care solution as a whole. The new risks are prefixed with EMIS XA.

	Risk description	Likelihood	Consequence / Impact	Risk Rating/ Score After mitigation actions implemented
EMIS XA 1	A confidentiality breach associated with the additional data in the feed.	Unlikely	Minor	Low
EMIS XA 2	The data in the feed from Connected Care into practices' EMISweb systems is attached to the wrong patients' records.	Unlikely	Moderate	Low
EMIS XA 3	A technical security failure with the additional EMIS XA data feeds.	Unlikely	Moderate	Low
EMIS XA 4	A technical quality failure with the additional EMIS XA data feeds.	Possible	Moderate	Low
CC Risk No. 1a	Breach of confidentiality – unlawful access to record (by staff)	Unlikely	Minor	Low
CC Risk No. 1b	Breach of confidentiality – unlawful access by external party	Unlikely	Minor	Low

Risk description		Likelihood	Consequence / Impact	Risk Rating/ Score After mitigation actions implemented
CC Risk No. 3	Alteration of data due to system process failure or technical security failure	Unlikely	Minor	Low
CC Risk No. 7	Unlawful processing or sharing of data	Unlikely	Major	Low
CC Risk No. 8	Loss of data (temporary or permanent), due to technical / security failure	Unlikely	Major	Low
CC Risk No. 19	Processes to respond to individual rights requests are insufficient (i.e. Subject Access)	Possible	Minor	Low
CC Risk No. 20	Poor quality data impacting on quality of care delivery	Possible	Minor	Low
CC Risk No. 28	Individuals are inadequately informed and compromised in exercising their rights	Possible	Moderate	Low
CC Risk No. 29	Excessive processing of data	Possible	Moderate	Low

Measures to reduce risks

Risk description		Measures to reduce, or remove risk	Effect on risk	Residual risk	Measure approved? Y/N
XA1	A confidentiality breach associated with the additional data in the feed.	• The measures used for Connected Care as a whole have the same ability to mitigate this risk	Likelihood reduced to 1	Low	Yes
XA2	The data in the feed from Connected Care into practices' EMISweb systems is attached to the wrong patients' records.	• The data extraction, transfer and upload processes at the EMIS end of the link will have been subjected to extensive testing and checks before being made operational • The data extraction, transfer and upload processes at the Graphnet Connected Care end of the link will be subjected to similarly extensive testing and checks before being made operational	Likelihood reduced to 1	Low	Yes
XA3	A technical security failure with the additional EMIS XA data feeds.	• The data extraction, transfer and upload processes at the EMIS end of the link has been subjected to extensive testing and checks before being made operational • The data extraction, transfer and upload processes at the Graphnet Connected Care end of the link will be subjected to similarly extensive testing and checks before being made operational	Likelihood reduced to 1	Low	Yes
XA4	A technical quality failure with the additional EMIS XA data feeds.	• The data extraction, transfer and upload processes at the EMIS end of the link has been subjected to extensive testing and checks before being made operational • The data extraction, transfer and upload processes at the Graphnet Connected Care end of the link will be subjected to similarly extensive	Likelihood reduced to 1	Low	Yes

	Risk description	Measures to reduce, or remove risk	Effect on risk	Residual risk	Measure approved? Y/N
		testing and checks before being made operational			
1a	Breach of confidentiality – unlawful access to record (by staff)	• Single Sign on – launch from patient record in operational system – reduced ability to 'browse' records. • Training for all staff • Employment contracts • Professional registration • Audit trail & disciplinary action - deterrent	Likelihood reduced to 1	Low	Yes
1b	Breach of confidentiality – unlawful access by external party	• Data centre security, inc physical access restrictions, network security features, penetration testing, vulnerability scans • End user premises security and system log on security	Likelihood reduced to 1	Low	Yes
3	Alteration of data due to system process failure or technical security failure	• Data extraction & upload process testing and checks • Training of Graphnet support staff • Data centre security, inc physical access restrictions, network security features, penetration testing, vulnerability scans	Likelihood reduced to 1	Low	Yes
7	Unlawful sharing of data	• Governance processes including DPIA, Sharing Framework and IG steering group reviewing all developments and ensuring all uses of data are conducted lawfully	Likelihood reduced to 1	Low	Yes
8	Loss of data (temporary or permanent), due to technical security failure	• Data centre security, inc physical access restrictions, network security features, penetration testing, vulnerability scans • Data Centre resilience arrangements, backups, fall back plans	Likelihood reduced to 1	Low Score	Yes
19	Processes to respond to individual rights requests are insufficient (i.e. Subject Access)	• Processes for items such as SARS have been set out, but requests are infrequent • Organisational requirements to support identified in the Regional Information Sharing Framework and part of the qualifying standard	Likelihood reduced to 1	Low	Yes
20	Poor quality data impacting on quality of care delivery	• Checks during design, extraction and upload processes • Visibility of data to wider user base • Reporting of queries	Likelihood reduced to 1	Low	Yes
28	Individuals are inadequately informed and compromised in exercising their data protection rights	• Qualifying standard requiring participating organisations to meet baseline 'informing' requirements. • Audits on compliance by partners • Common statements shared, common web resources	Likelihood reduced to 1	Low	Yes
29	Excessive processing of data	• Datasets extracted have been subjected to clinical review and are identified as necessary for the effective delivery of care across the health & care community • QC review of approach and repository based data sharing • Role Based Access to reduce access to data in repository to data items identified as needed by user role	Likelihood reduced to 1	Low	Yes

End of Schedule L