{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – PC180005 – Federated Working (Berkshire West):

Schedule K – Processing and Sharing Specification (signature required)
Schedule L – Initial Data Protection Impact Assessment (if a DPIA was not required) or Data Protection Impact Assessment Summary (if a DPIA was required)

Variable information managed by the Administrator:

Schedule C – Direct Care Sharing Register (List of shared data flows)
Schedule D – Other (Secondary) Uses Sharing Register (List of shared data flows)
Schedule E – Membership Register (List of participating organisations)
Schedule F – Shared Information Asset Register
Schedule G – Approved Generic Use Cases for Shared Information
Schedule H – Approved Generic Privacy and Processing Notices

Sharing Agreement Narrative and Guidance

Visit www.regisa.uk for the narrative and the latest version of Schedules C-H

Schedule K – PC180005 – Federated Working (Berkshire West)

Sharing Requirement Identifier:	PC180005
Sharing Requirement Name:	Federated Working (Berkshire West)
Sharing Requirement Start Date:	01 August 2018
Sharing Requirement End Date:	30 April 2023
Sharing Organisation:	{{!org_es_:font(name=calibri,size=10) }}
Direct Care or Other Uses:	Direct care
Risk Sharing and Indemnity:	Out of scope
Sharing Data Controllership:	Joint control with NHS Berkshire West CCG as lead controller
Data Processor(s):	TPP - EMIS - INPS
Status:	Active
Version:	v4

Summary of the Sharing Requirement Purpose

The Berkshire West extended hours and federated working solution enables medical records from a patient's registered practice to be electronically shared and made available to alternative practices providing primary care services outside of core hours. These alternative practices that provide services outside of the core hours are referred to as "hub practices" and the medical records are known as the "shared record".

The purpose of the extended hours solution is to ensure that the care provided outside of the core hours by the hub practices is safe and consistent with patients' existing risks, diagnoses, conditions, problems, medication and other treatment.

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.

Summary of the Sharing Requirement Process

For the purposes of the extended hours solution, the practices are organised into primary care alliances with practices within each alliance providing hub practice services on a rotating basis to the other practices in the alliance. Practices providing hub services may provide services to any practice within the alliance. The organisation of the alliances, localities and clusters is identified in Table 1 below.

The extended hours solution sharing process is as follows:

1. At the time a patient requests an extended hours appointment, the patient's registered practice uses the Vision 360 application to identify available appointments at the extended hours hub practice and an appointment is chosen and then allocated to the patient concerned;
2. At the time of the extended hours appointment itself, the patient's record as held in the patient's registered practice clinical system is accessed from the hub practice by the consulting clinician as outlined in paragraphs 5-8 below;
3. Once the patient consultation is completed, the consultation detail is either recorded directly into or transferred into the patient's registered practice clinical system; and
4. Where actions cannot take place at the time of the consultation or where agreement to a proposed course of action needs to be deferred to the registered practice, the consulting clinician uses the task delegation capability of the clinical system concerned to delegate and request follow-up actions in the patient's registered practice.

The platform for the extended hours solution comprises:

5. EMISweb:
    a. For consultations involving patients registered with EMISweb based practices and attending a consultation at EMISweb based hub practices, either:
        i. EMIS Switch allows authorised personnel in the hub practice to access the patients' registered practice clinical system - thereby enabling full record access and the delivery of high quality patient care
        ii. Or the Vision Anywhere solution enables access to the patients' clinical record to conduct the consultation;
6. Vision:
    a. For consultations where INPS Vision is the clinical system, either at the patients' registered practice or at the hub site, the Vision Anywhere solution enables access to the patients' clinical record to conduct the consultation;
7. SystmOne:
    a. For consultations involving patients registered with TPP SystmOne practices and attending a consultation at TPP SystmOne based practices, TPP SystmOne allows authorised personnel in the hub practice to access the patients' registered practice clinical system - thereby enabling full record access and the delivery of high quality patient care
    b. For consultations where TPP SystmOne is the clinical system at just one of:
        i. the patient's registered practice
        ii. the hub practice where the consultation occurs

    access to patients' clinical records is achieved using Remote Desktop. With Remote Desktop, authorised personnel in the hub practice use the Remote Desktop solution to login to the clinical system at the patient's registered practice to access the clinical records and to conduct the consultation
8. And for any practices that have an agreement to do so (in particular Peppard Road), patients registered at the practice are offered the opportunity to make a booked appointment to be seen at Reading Walk In Centre;
9. For practices with access to the GP Connect solution, GP Connect may also be used to support consultations;
10. Docman 7, 10 and Docman Share can be used to view clinical documents held in Docman clinical document repositories;
11. Records are securely accessed over HSCN/N3 IGSoC approved system by means of a tried and proven data sharing process that is accredited by the GP clinical system suppliers; and
12. In all cases full write back capability is enabled to provide a secure and safe history of the encounter to be recorded in the patients' clinical records at their registered practice.

Summary of the Sharing Requirement Privacy Arrangements

The privacy arrangements are considered satisfactory as:

1. Access to view data is managed in accordance with RBAC (Role Based Access Control) arrangements where:
    a. Only personal demographic data can be viewed by non-clinical roles
    b. Sensitive and confidential data may only be reviewed by clinical roles
    c. A legitimate relationship exists between the patient and the person accessing the data;

2. The data is accessed in accordance with the opt-out consent model as summarised by points 3 and 4 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. Data items are not made available for sharing where a practice has indicated that the sensitive diagnoses and data items concerned are not to be shared;
5. An audit trail is available showing which user accessed a data subject's records; and
6. While the individual in the patient's registered practice who is making the booking can choose from all patients within the alliance concerned when making a booking, only demographic data is accessible and viewable.

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 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.

Table 1 – Sharing and User Organisation Arrangements

For the purposes of this sharing requirement the user organisations also include Reading Primary Care Alliance Ltd where Reading Primary Care Alliance Ltd is contributing to or coordinating patient care.

For the purposes of this sharing requirement the hub practice user organisations and Reading Primary Care Alliance Ltd may create, edit and view patient personal confidential data for patients registered in any of the practices identified above in respect of consultations provided on behalf of the patient's registered practice.

The practice organisations identified in Table 1 below agree 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.

The sharing practices below from time to time perform the role of hub practice for the rest of the practices identified in the alliance concerned. Hub practices may also from time to time perform the hub role for any practice identified in Table 1.

Table 1 identifies each of the Berkshire West extended hours alliances, localities and clusters and for each the participating practices are listed. The primary clinical system used is presented below for each practice.

Alliance	Locality	Cluster	Practice	Clinical System
Newbury and Villages	Newbury & District	Newbury	Burdwood Surgery	INPS Vision
			Chapel Row Surgery	EMISweb
			Eastfield House Surgery	EMISweb
			Falkland Surgery	EMISweb
			Hungerford Surgery	TPP SystmOne
			Kintbury & Woolton Hill Surgery	EMISweb
			Lambourn Surgery	TPP SystmOne
			Strawberry Hill Medical Centre	EMISweb
			Thatcham Health Centre	INPS Vision
			The Downland Practice	EMISweb
	North & West Reading	Villages	Mortimer Surgery	INPS Vision
			The Boat House Surgery	EMISweb
			Theale Medical Centre	EMISweb
Reading Primary Care Alliance	North & West Reading	Caversham	Balmore Park Surgery	EMISweb
			Emmer Green Surgery	EMISweb
			Peppard Road Surgery	TPP SystmOne
		Reading West	Circuit Lane Surgery	EMISweb
			Tilehurst Surgery	EMISweb
			Western Elms Surgery	EMISweb
	South Reading	South Reading Central	Abbey Medical Centre	EMISweb
			Chatham Street Surgery	EMISweb
			Dr M L Swami & Partners	INPS Vision
			Eldon Road Surgery	EMISweb
			Kennet Surgery	EMISweb
			Melrose Surgery	EMISweb
			Pembroke Surgery	INPS Vision
		Tilehurst	Grovelands Medical Centre	EMISweb
			Tilehurst Village Surgery	EMISweb
			Westwood Road Surgery	EMISweb
		Whitley	Dr Mittal & Partners	EMISweb
			London Street Surgery	EMISweb
			Long Barn Lane Surgery	EMISweb
			South Reading Surgery	INPS Vision
			University of Reading Medical Practice	EMISweb
	Wokingham	West	Brookside Practice	INPS Vision
			Finchampstead Practice	EMISweb
			Swallowfield Medical Practice	INPS Vision
		North	Loddon Vale Practice	EMISweb
			Parkside Practice	EMISweb
			Twyford Practice	INPS Vision
			Wargrave Practice	INPS Vision
			Wilderness Practice	EMISweb
			Woodley Practice	EMISweb
		East	Burma Hill Practice	EMISweb
			New Wokingham Road Surgery	EMISweb
			Wokingham Medical Centre	EMISweb
			Woosehill Medical Centre	EMISweb

End of Table 1 – Sharing and User Organisation Arrangements

The Shared Categories of Data

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

1. Person Details and Demographics;
2. Allergies and Adverse Reactions;
3. Care and Management Plans;
4. Clinical Correspondence;
5. Consultations;
6. Events and Encounters;
7. Examinations;
8. Health Promotion;
9. Immunisations;
10. Medications;
11. Preferences and Lifestyle;
12. Problems;
13. Procedures;
14. Referrals Details;
15. Risks and Alerts;
16. Screening;
17. Social / Family History; and
18. Tests and Results.

The above categories of data include both coded data as well as free text.

For all categories of data, the primary data controller is the registered practice and the application that is the source of the data is the GP system at the patient's registered practice.

While a sharing agreement is only necessary for information regarded as personal confidential data, some of the data identified above is included for the purpose of completeness not because the data is regarded as personal confidential data.

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.1 Excluded Read Codes.

Summary of the Initial Data Protection Impact Assessment

The 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. There is sharing of data through multiple stakeholders who utilise appropriately secured communication channels.

The users of this information would normally be expected to have access to this level of personal information as part of their normal working environment.

The Initial Data Protection Impact Assessment, which has been answered objectively, indicates that no material and unmitigated information risks are generated by the extended hours solution and as a consequence a full Data Protection Impact Assessment is not required before sharing can occur.

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, for and
on behalf of {{!org_es_:font(name=calibri,size=10) }}
{{!addr_es_:font(name=calibri,size=10) }}.

Annex D.1 – Excluded Read Codes

The table below summarises the Read codes that are excluded when Shared Record data is sourced from the general practice clinical systems.

Description	Category / Code
HSA1-Therap. Abort. Green Form	956%
Suction Termination Of Pregnancy	7E084%
Termination Of Pregnancy NEC	7E086%
Legally Induced Abortion	L05%

End of Schedule K

Schedule L – PC180005/{{!dpiaprefix_es_:font(name=calibri,size=10)}}– Federated Working (Berkshire West)

This schedule to the Regional Health and Social Care Information Sharing Agreement provides 14 questions covering five risk categories which when answered objectively offer an initial assessment of the additional risks to privacy posed by the proposed sharing of information.

Where a question gives rise to an affirmative answer, it does not automatically follow that a full scale Data Protection Impact Assessment is required. Each affirmative answer needs to be assessed for materiality (probability and impact) and for ways in which the potential risks can be avoided or materially mitigated with a revised solution or additional measures.

Where a substantial number of questions give rise to an affirmative answer this is a good indicator that a full scale Data Protection Impact Assessment is required and project plans should include the costs and timescales of this activity and any associated consultation that may be needed.

Wherever practical the rationale for an answer should be included with the answer.

Questions relating to "identifying data" and "identification" (questions 3, 5 and 7 to 11) are of heightened importance in the context of Provision of Care for data that has not been anonymised or pseudonymised.

These questions are derived from guidance provided by the Information Commissioner's Office and from the Information Governance Alliance (*Integrated Digital Care Records: Data Controller Issues*).

Technology Risk

1. Does the proposed change apply new or additional information technologies that have substantial potential for privacy intrusion? … **No. The core new technologies have been tried and proven over several 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 previous methods such as printed records, fax, letter and multiple systems.**

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.**
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 use of identifiable information is necessary to provide care to patients. This is unchanged.**

Organisational Risk

4. Does the proposed change involve multiple organisations that do not have a prior history of working together and sharing information? … **No.**
5. Does the proposed change involve data processor organisations that do not have a prior history of working with similar shared information? … **No. The organisations concerned have considerable history of working together in the provision of care. The organisation risk level is considered low as the job functions, roles and confidentiality requirements are the same across all organisations and the sharing arrangements are based on standard datasets with confidentiality requirements that are understood by all involved.**
6. 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.**

Data Risk

7. Does the proposed change involve new or significantly changed handling of identifying data that is of particular concern to individuals? … **No. This is a continuation of a previous sharing arrangement and the technology is tried and proven and the categories of data that are being shared would normally be shared or be available for sharing for consultations and the provision of care by other healthcare organisations.**
8. Does the proposed change involve new or significantly changed handling of a considerable amount of identifying data about each individual in the database? … **No. The data can only be shared on a person by person basis and only after the data users have logged in with secure patient access credentials.**
9. Does the proposed change involve new or significantly changed handling of personal data about a large number of individuals? … **No. The data can only be shared on a person by person basis and no bulk data access is available.**

10. Does the proposed change involve new or significantly changed consolidation, inter-linking, cross referencing or matching of identifying data from multiple sources? … **No. The only patient data accessed during a consultation is held in the EMIS Web system and in the DocMan system (for attachments).**
11. Does the proposed change involve the creation of new data outside of the boundaries of the existing source systems? … **No. This is a continuation of a previous sharing arrangement and the technology is tried and proven and the categories of data that are being shared and created would normally be created or be available for sharing for consultations and the provision of care by other healthcare organisations.**

Exemption and Exclusion Risk

12. Does the proposed change relate to data processing which is in anyway exempt from legislative privacy protections? … **No.**
13. Does the proposed change's justification include significant contributions to public security measures? … **No.**
14. 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.**

End of Schedule D