{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – PC170003 – Bracknell and Ascot GP Extended Hours and Integrated Urgent Care Pathway:

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)

Sharing Agreement Narrative and Guidance

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

Schedule K – PC170003 – Bracknell and Ascot GP Extended Hours and Integrated Urgent Care Pathway

Sharing Requirement Identifier:	PC170003
Sharing Requirement Name:	Bracknell and Ascot GP Extended Hours and Integrated Urgent Care Pathway
Sharing Requirement Start Date:	01 April 2021
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 Frimley CCG as lead controller
Data Processor(s):	EMIS
Status:	Active
Version:	v3

Summary of the Sharing Requirement Purpose

The Bracknell and Ascot extended hours solution and integrated urgent care pathway enables information about a patient's medical condition to be electronically shared and made available to organisations acting as extended hours and integrated urgent care pathway providers. The platform for the solution is the EMIS Web for Clinical Services (EMIS CS) product. Once configured to allow the necessary cross practice functions in each practice, EMIS CS provides a N3 IGSoC approved system that allows secure cross practice access to patient information held in patient's GP records.

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

The EMIS CS cross organisational sharing, tasks and appointment booking features are used to allow users to add and cancel appointments in other organisations' appointment books and to create appropriate consultation and follow-up, review and audit tasks. As a consequence:

1. Extended hours and integrated urgent care pathway provider users are able to send tasks to users at the patient's registered practices;
2. Registered practices are able to book appointments in the shared appointment book and send tasks to configured users at the extended hours and integrated urgent care pathway providers;
3. Patients' records are shared with the clinicians working at the extended hours and integrated urgent care pathway providers;

4. Patient consultations recorded by the extended hours and integrated urgent care pathway providers are shared with the patient's registered practice;
5. Patients' registered practice records are updated by the extended hours and integrated urgent care pathway provider clinical summariser to reflect consultations and to complete 2 week wait referrals as and when necessary; and
6. For practices with access to the GP Connect solution, GP Connect may also be used to support consultations and the booking of appointments.

The categories of data to be shared are summarised below.

Where a patient's extended hours or integrated urgent care pathway consultation occurs in a practice other than the patient's registered practice, the details of the consultation are recorded in the EMIS Web system of the practice providing the consultation as well as within the patient's registered practice.

On completion of the consultation by the extended hours and integrated urgent care pathway providers the saved data is exported to the patient's registered practice by EMIS CS and after review in the registered practice it is imported to form part of the patient's primary record.

The extended hours and integrated urgent care pathway provider clinical summariser will record read coded entries to capture new diagnosis and general outcomes of consultations, inclusive of completing 2 week wait referral process at the patient's 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 and consent model as summarised by points 3, 4 and 6 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. Consent to view a patient's record is implied where the patient concerned presents at their registered practice and at a practice other than the patient's registered practice. As a consequence, explicit consent to access the patient's data is not requested during the consultation itself.

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 and extended hours and integrated urgent care pathway provider 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 Shared Categories of Data

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

The shared data categories are represented by the following EMIS modules:

1. Patient demographic and identifying details
2. Summary information
3. Consultations
4. Medication
5. Problems
6. Investigations
7. Care history
8. Diary and appointments
9. Documents and attachments
10. Referrals
11. Warnings

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.

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.

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, has not identified any major risks and consequently it is considered that there are no significant privacy risks in relation to this proposed change. Consequently the intended change and use of associated data is considered an acceptable risk and in the public interest of improving care planning and making patient preferences more widely known to those involved in healthcare provision.

A detailed Data Protection Impact Assessment is not required.

See the attached Initial Data Protection Impact Assessment.

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) }}.

End of Schedule K

Schedule L – PC170003 – Bracknell and Ascot GP Extended Hours and Integrated Urgent Care Pathway

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.**

Summary of the Initial Data Protection Impact Assessment

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

A 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, has not identified any major risks and consequently it is considered that there are no significant privacy risks in relation to this proposed change. Consequently the intended change and use of associated data is considered an acceptable risk and in the public interest of improving care planning and making patient preferences more widely known to those involved in healthcare provision.

A DPIA has not been conducted.

End of Schedule L