

DATA SHARING AGREEMENT FOR EXTENDED ACCESS SERVICE HUBS FOR PRIMARY CARE ACROSS STAFFORDSHIRE AND STOKE ON TRENT

CONTENTS

1. Policy Statements and Purpose of this Data Sharing Agreement.....	3
2. Legal Basis for Data Sharing.....	4
3. Data	5
3.1 What data is it necessary to share?	5
3.2 Who is going to be responsible for sharing this data and ensuring data is accurate?	6
3.3 How will you keep a record of what data has been shared?	7
3.4 How is this data going to be shared?	7
3.5 Who will have access to this data and what may they use it for?	8
3.6 Timescales.....	9
3.7 How securely does the data need to be stored?	9
3.8 How long are you going to keep the data?	10
3.9 Further Use of Data.....	10
4. Breach of confidentiality.....	11
5. Complaints procedures.....	11
6. Access to Information	12
7. Review of Data Sharing Agreement.....	12
8. FREEDOM OF INFORMATION ACT (2000) (foia).....	13
9. CLOSURE/TERMINATION OF AGREEMENT	13
10. Signatories	14
Appendix A – Parties to the agreement	15
Appendix B – EMIS Remote Consultation Configuration Request	19
Appendix C – The MIG Data Sharing Agreement	22

1. POLICY STATEMENTS AND PURPOSE OF THIS DATA SHARING AGREEMENT

The objective of this agreement is to enable the teams working within the Northern Staffordshire GP Federation, the East Staffordshire Primary Care Partnership, the Mercian GP Network, GP First, Cannock Chase Clinical Alliance and Lichfield and Burntwood GP Network (referred to as the Extended Access Service hub) to have access to the general practice record of patients registered with the named practices within this agreement located at Appendix A of this document. This will enable patients to receive;

- Additional appointments Monday to Friday (up until 8pm), at weekends and on bank holidays at sites other than their own GP Practice (Requirement of the GP Forward View for CCGs to commission extended access to Primary Care which involves additional appointments between 8am and 8pm)
- More informed care, resulting in a higher quality of care
- Improved safety
- Better outcomes for patients including experience.

Clinicians working within the parties named above will access patient records via the EMIS clinical system which is a nationally recognised GP system of choice. The information available for sharing will be the EMIS electronic patient records of patients registered at the GP practice and thereby patient identifiable information. The parties will be able to access any patient record from any of the GP practices listed in Appendix A of this document.

The EMIS clinical system will provide the data to the extended access service hub and this will be via EMIS Web Clinical Services and EMIS Remote Consultations solutions. EMIS EPR Viewer will be used for practices using TPP SystmOne.

It is anticipated that an IT solution will be available which will enable record sharing between GP System of Choice Principle (GPSoc) suppliers (TPP SystmOne, EMIS clinical systems, INPS Vision and Microtest) where locally required. Access to this will be made available through the EMIS Clinical Service system used to provide services in each area.

Where available, Docman Share will be used to share patient documents between the patients practice and the service they are linked to on a cloud.

Within this agreement all GP practices will be both the data controller and EMIS will be the data processor for the data.

An additional solution will also be used where areas have a mixed GP clinical system estate. The Medical Interoperability Gateway (MIG) will be used to provide the following non-EMIS data to extended access service hub to support safe delivery of care:

MIG Detailed Care Record

- Patient Demographics
- Summary, including Current Problems, Current Medication, Allergies, and Recent Tests
- Problem view
- Diagnosis View
- Medication including Current, Past and Issues

- Risks and Warnings
- Procedures
- Investigations
- Examination (Blood Pressure Only)
- Events consisting of Encounters, Admissions and Referrals

The purpose of this is to provide integration of the GP Detailed Care Record (DCR) service from practices in East Staffordshire CCG to the East Staffordshire Primary Care Partnership respectively.

Healthcare Gateway will provide the MIG technology and hosting infrastructure to support the interoperability between provider (sharing) organisations and consumer (viewing) organisations. The sharing of records allows a read only access to the Extended Access Service Hub at the point of care; they will be unable to write directly into the consultations and / or patient record.

Information available to clinicians via these digital solutions should only be accessed when verbal consent is given by the patient and this will be recorded against the patient's record at the point where their registered practice books an appointment or during a consultation with the Extended Access Service Hub.

2. LEGAL BASIS FOR DATA SHARING

This Data Sharing Agreement has been developed to achieve the objectives as set out in Section 1. It is the intention that all aspects of information sharing and disclosure relating to this agreement shall comply with legislation that protects personal data.

The data will be shared for the purposes of enabling direct care to any patient registered at a GP Practice detailed in Appendix A of this document. Therefore, under Data Protection Act 2018 (DPA18) / General Protection Data Regulation (GDPR), the data will be shared under the following conditions for processing:

- **Article 6 (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. Put full title of articles in for 6 and 9
- **Article 9 (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.

Patients have rights under DPA18 / GDPR, which include:

- 1) The right to be informed
- 2) The right of access
- 3) The right of rectification
- 4) The right to erasure ('right to be forgotten')
- 5) The right to restrict processing
- 6) The right to data portability
- 7) The right to object
- 8) Rights of automated decision making and profiling

3. DATA

3.1 WHAT DATA IS IT NECESSARY TO SHARE?

The data to be shared between the GP Practices and the parties listed and their associated staff and back again will be the full clinical record of the patient and therefore patient identifiable data. This will include the patient's name, home address including post code, date of birth, contact number, NHS number, gender, full medical history and ethnicity. This is to enable the patient to access the extended access service hub and to have an appointment at another site other than their own GP Practice. To allow staff working for the parties listed to view the patient clinical records, will enable them to provide the patient with the most appropriate clinical care, which is more informed, resulting in a high quality of care, improved safety and better outcomes, including patient experience. Reception staff at the identified sites will have role-based access with restricted access so will not be able to see medical details.

Data Set	Who from	Who to	Which Organisation owns the information (Who is the Data Controller?)	Frequency of Sharing
EMIS Remote Consultations Full clinical record including full medical history incl name, DOB, address, postcode, contact no, NHS number, Gender & Ethnicity	GP Practices	North Staffordshire GP Federation East Staffordshire Primary Care Partnership The Mercian GP Network GP First Cannock Chase Clinical Alliance Lichfield & Burntwood GP Network	GP Practices	When the patient registered with the GP Practices has an appointment within the extended access service hub
Medical Interoperability Gateway (MIG) Information to be shared: Patient Demographics, Summary, including Current	GP Practices	East Staffordshire Primary Care Partnership	GP Practices	When the patient registered with the GP Practices has an appointment within the extended access service hub

Problems, Current Medication, Allergies, & Recent Tests, Problem view, Diagnosis View, Medication including Current, Past & Issues, Risks and Warnings, Procedures, Investigations, Examination (BP Only), Events consisting of Encounters, Admissions & Referrals				
Docman Share Patient clinical and discharge letters	GP Practices	North Staffordshire GP Federation East Staffordshire Primary Care Partnership The Mercian GP Network GP First Cannock Chase Clinical Alliance Lichfield & Burntwood GP Network	GP Practices	When the patient registered with the GP Practices has an appointment within the extended access service hub

It is each data controller's responsibility to update and publicise their own practice Privacy notices.

3.2 WHO IS GOING TO BE RESPONSIBLE FOR SHARING THIS DATA AND ENSURING DATA IS ACCURATE?

The GP Practice to which the patient is registered is responsible for sharing the patient's data to the parties listed and their associated staff to enable the patient to have an appointment within the extended access service hub. All data recorded on the clinical system will be maintained and recorded accurately by identified members of staff within the GP Practice relating to their roles and responsibilities i.e. administration staff, clinical staff and so on.

The listed parties and their associated staff are also responsible for ensuring accurate data is recorded within the clinical system when they have a patient with an appointment at the extended access service hub to ensure correct clinical data is reported back to the patients registered GP Practice following their appointment.

3.3 HOW WILL YOU KEEP A RECORD OF WHAT DATA HAS BEEN SHARED?

Within EMIS Remote Consultations, the following information is available for auditing:

- Whether consent has been provided for an external clinician viewing and recording into the patient's GP record when the patient's own registered GP practice books them an appointment to be seen at a different practice / hub
- Appointments – recorded in the system audit trail – both the patient's registered organisation and the consulting organisation can view the audit trail for any externally booked appointment slots as well as those booked by their own organisation – can view full details and export data
- When the clinician at the Extended Access Service Hub accesses the patient's registered GP record, all activity is audit trailed on the patient's registered GP system
- Consultation History Page – can click on individual consultations for the patient and shown a full audit trail of changes etc to that consultation

Within Docman Share, it maintains a log at a database level of who has accessed the patient letters.

Within the MIG, the audit trail available consists of the following:

- Name of the clinician who has viewed the patients record
- The viewing organisation
- Date and time the record was accessed

3.4 HOW IS THIS DATA GOING TO BE SHARED?

Data is going to be shared between the GP Practices and the Extended Access Service Hub by using EMIS Web Clinical System and EMIS remote consultations. This will function with all the practices that currently have EMIS Web as their chosen clinical system. The EMIS Web clinical system will provide the data to the Extended Access Service Hubs and this will be via EMIS Web Clinical Services and EMIS Remote Consultations solutions. EMIS EPR Viewer will be used for practices using TPP SystemOne.

An additional solution will also be used where areas have a mixed GP clinical system estate (TPP, Vision or Microtest – East Staffordshire). The Medical Interoperability Gateway (MIG) will be used to allow the sharing of data between the GP clinical system and the Extended Access Service Hub with the following information to support the safe delivery of care:

MIG Detailed Care Record

- Patient Demographics
- Summary, including Current Problems, Current Medication, Allergies, and Recent Tests
- Problem view
- Diagnosis View

- Medication including Current, Past and Issues
- Risks and Warnings
- Procedures
- Investigations
- Examination (Blood Pressure Only)
- Events consisting of Encounters, Admissions and Referrals

Healthcare Gateway will provide the MIG technology and hosting infrastructure to support the interoperability between provider (sharing) organisations and consumer (viewing) organisations. The sharing of records allows a read only access to the Extended Access Service Hub at the point of care; they will be unable to write directly into the consultations and / or patient record therefore the consultations will be recorded in the EMIS Hub system of the Extended Access Service Hub.

EMIS Web, TPP, Vision and Microtest are secure online patient systems that are used across most of the UK. All data will be contained within the clinical system which have strict security measures to protect the data - these measures are regularly audited to ensure that the stringent processes are maintained.

A further solution is Docman Share. This will be used to share patient documents between the patients practice and the service they are linked to on a cloud. The patient's documents will be securely hosted by Docman in line with the NHS digital secure standards they are mandated to deliver solutions to. Documents are then only presented to a clinician as and when they have been given verbal consent to access the patient's record. If consent is refused, the data will not be accessible by anyone other than the practice the patient is registered with. Practices not using Docman will now share documents via the Docman Share solution.

Information available to clinicians via these digital solutions should only be accessed when verbal consent is given by the patient and this will be recorded against the patient's record at the point where their registered practice books an appointment or during a consultation with the Extended Access Service Hub.

3.5 WHO WILL HAVE ACCESS TO THIS DATA AND WHAT MAY THEY USE IT FOR?

Staff are granted role-based access and restrictive access based on their role and their need to access information. All employees with access to patient data will be bound by the NHS code of confidentiality with confidentiality clauses embedded into contracts. All members of staff who use a smartcard to access patient records have to sign an RA01 form and are also bound by the NHS Code of Confidentiality contained within the standard NHS employee contract. The Extended Access Service Hub will undertake regular privacy audits for information governance purposes relating to appropriate access by the Extended Access to Primary Care Service to patient records.

Access to this data will enable the patient to access the extended access service hub and to have an appointment at another site other than their own GP Practice. For the Extended Access Service Hub to view the patient clinical records, it will enable them to provide the patient with the most appropriate clinical care, which is more informed, resulting in a high quality of care, improved safety and better outcomes, including patient experience. Reception staff at the identified sites will have role-based access with restricted access so will not be able to see medical details.

NHS 111 will be able to book appointments via the clinical systems appointment book into the extended access service hubs but will not have access to any clinical records and may have access to summary care records - questions can be asked by NHS 111 to enable them to triage effectively and provide a relevant appointment.

If any patient no longer wishes their record to be available to the extended access service hub, they need to inform their GP practice and the GP practice will then inform the clinical system provider who will remove access to that patient's record. If this was the case, the patient would no longer be able to receive appointments through the extended access service hub but their rights to object and withdraw would be respected.

3.6 TIMESCALES

Data will be shared for an individual patient each time they have an appointment within an extended access service hub. The contract for this service is for 3 years, between 1st September 2018 and 31st August 2021.

3.7 HOW SECURELY DOES THE DATA NEED TO BE STORED?

GP practices have strict policies for its staff to follow regarding access to IT equipment, including not sharing passwords and log in details; these procedures will be applied to the extended access service hub environment. Patient records are only accessible on the clinical system via a smartcard which requires the use of a 4-digit pin. Care must be taken by everyone issued with a smartcard to keep it secure and protect their pin against discovery and cards should be treated with care and protection to prevent any loss or damage.

Staff must not leave smartcards in computers

Smartcards should never be left unattended. Staff must take all reasonable steps to ensure that workstation's are always left secure when not in use by removing Smartcards however briefly the workstation is left unattended. Never leave your Smartcard in the Smartcard reader when you are not actively using it.

Any lost or stolen cards should be reported immediately to your sponsor and registration authority agent so they can cancel your card and replace it as soon as possible.

Please note that the terms and conditions of smartcard usage is monitored and when an employee signs up to the terms and conditions laid out on the RA01 form, the following condition is agreed to:

By signing the declaration set out in the RA01 Short Form, I, the applicant: acknowledge that my Smartcard may be revoked or my access profiles changed at any time without notice if I breach this Agreement; if I breach any guidance or instructions notified to me for the use of the NHS Care Records Service applications or if such revocation or change is necessary as a security precaution. I acknowledge that if I breach this Agreement this may be brought to the attention of my employer (or governing body in relation to independent contractors) who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution);

Therefore, any breaches of these terms and conditions will be treated as a disciplinary offence under the organisations disciplinary procedure.

EMIS Web, TPP, Vision and Microtest are secure online patient systems that are used across most of the UK. All data will be contained within the clinical system which have strict security measures to protect the data - these measures are regularly audited to ensure that the stringent processes are maintained. Reception staff at

the identified sites will have role-based access with restricted access so will not be able to see medical details.

Docman Share will be used to share patient documents between the patients practice and the service they are linked to on a cloud. The patient's documents will be securely hosted by Docman in line with the NHS digital secure standards they are mandated to deliver solutions to. Documents are then only presented to a clinician as and when they have been given verbal consent to access the patient's record. If consent is refused, the data will not be accessible by anyone other than the practice the patient is registered with. Practices not using Docman will now share documents via the Docman Share solution.

The Medical Interoperability Gateway (MIG) will be used to allow the sharing of data between the GP clinical system and the Extended Access Service Hub. Healthcare Gateway will provide the MIG technology and hosting infrastructure to support the interoperability between provider (sharing) organisations and consumer (viewing) organisations. The sharing of records allows a read only access to the Extended Access Service Hub at the point of care; they will be unable to write directly into the consultations and / or patient record therefore the consultations will be recorded in the EMIS Hub system of the Extended Access Service Hub.

NHS 111 will be able to book appointments via the clinical systems appointment book into the extended access service hubs but will not have access to clinical records and may have access to summary care records - questions can be asked by NHS 111 to enable them to triage effectively and provide a relevant appointment.

If there is a security breach in which data received from another party under this agreement is compromised, the originator will be notified at the earliest opportunity via the post holder identified at 3.2.

The Extended Access Service Hub will undertake regular privacy audits for information governance purposes relating to appropriate access by the Extended Access to Primary Care Service to patient records.

3.8 HOW LONG ARE YOU GOING TO KEEP THE DATA?

The data recorded as part of the extended access service will form part of the medical records of that patient held by their registered GP practice. The retention period deemed applicable based on the NHS retention schedule (<https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>) is Care Records with standard retention periods, GP Patient Records, 10 years after death (also exceptions).

3.9 FURTHER USE OF DATA

There is no other use of this data; the data will be used for direct patient care only. Any parties using the data for purposes not specified in this data sharing agreement will be subject to an investigation and disciplinary procedures.

To support the Clinical Commissioning Groups (CCGs) in the commissioning of services, purely anonymised data will be used for contract monitoring purposes and to inform on commissioning decisions. The Extended Access Service Hub will provide data using an Excel document where the reporting requirements have already been outlined in their Extended Access Service contracts with the CCGs. This data will include:

- The number of patients seen through the extended access service hub and whether these were GP or Nurse appointments
- A summary showing percentage of each GP practices registered patients that have accessed the services and the type of service accessed.
- Percentage of patients having required access to interpretation services.
- Consultation / appointment outcomes i.e. referred to A&E, speciality referral, admitted to emergency portal.

4. BREACH OF CONFIDENTIALITY

The General Data Protection Regulation (GDPR) as implemented by the UK Data Protection Act 2018 came into UK Law on 25 May 2018. It introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The Security of Network and Information Systems Directive ("NIS Directive") also requires reporting of relevant incidents to the Department of Health and Social Care as the competent authority from 10 May 2018.

It is a legal obligation to notify personal data breaches of the General Data Protection Regulation under Article 33 within 72 hours, to the ICO, unless it is unlikely to result in a risk to the rights and freedoms of individuals. Article 34 also make it a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a high risk to individuals rights and freedoms. It is also a contractual requirement of the standard NHS contract to report incidents in accordance with this guidance. By notification this may be an initial summary with very little detail known at the outset but a fuller report that might follow. There is no expectation that a full investigation will be carried out within 72 hours. The Information Commissioner has asked all relevant health and social care organisations to use this reporting tool accessed via the Data Security and Protection Toolkit in preference to the ICO provided reporting mechanism so that sector intelligence gathering and local solutions to groups of incidents can be implemented.

A processor of personal data that discovers a breach has occurred has a legal obligation to inform the controller of that personal data under Article 33(2) of GDPR as clarified in the Article 29 working party guidelines on personal data breach reporting (II, A, 3). It is possible for a processor to make a notification on behalf of the controller, but only where the controller has authorised the notification and this has been documented as part of the contractual arrangements between the controller and the processor. However, it is important to note that the legal obligation remains with the controller.

All security breaches and breaches of confidentiality that fall within the criteria of reportable incidents that occur at the Extended Access Service Hub must be reported on the GP practices toolkit, to which the patient is registered at that GP practice or is the data controller for that patient. The individual GP / Nurse in the Extended Access Service hub that has caused the breach must notify the patient's registered GP Practice to advise of the breach and also report the incident on a breach tracker held centrally by the Extended Access Service hub.

The Guide to the Notification of Data Security and Protection Incidents which includes assessing the level of incident and likelihood of the risk to the personal rights and freedoms of individuals is available on the NHS Digital website <https://www.dsptoolkit.nhs.uk/Help/29>

5. COMPLAINTS PROCEDURES

Each partner must be committed to having procedures in place to address complaints relating to inappropriate disclosure or failure to disclose personal information. Any complaints made against this data sharing agreement will be dealt with by Midlands and Lancashire Commissioning Support Unit on behalf of Cannock Chase, East Staffordshire, North Staffordshire, Stoke-on-Trent, South East Staffordshire and Seisdon Peninsula and Stafford and Surrounds CCG's. Complaints shall be directed to the freepost address below.

Freepost

RTAA-XTHA-LGGC

Patient Plus

Midlands and Lancashire Commissioning Support Unit

Springfields Health & Wellbeing Centre

19 Lovatt Court

Rugeley

WS15 2FH

Freephone: 0800 030 4563

E-mail: mlcsu.patientservices@nhs.net

6. ACCESS TO INFORMATION

All recorded information held by public sector agencies is subject to the provisions of the Freedom of Information Act 2000 and the Data Protection Act 2018. While there is no requirement to consult with third parties under FOIA, the parties to this agreement will consult the party from whom the data originated and will consider their views to inform the decision making process. All decisions to disclose must be recorded by the disclosing organisation.

Each Partner Organisation shall publish this agreement on its website and refer to it within its Publication Scheme. If a Partner Organisation wishes to withhold all or part of the agreement from publication it shall inform the other Partner Organisations as soon as reasonably possible. Partner Organisations shall then endeavour to reach a collective decision as to whether information is to be withheld from publication or not. Information shall only be withheld where, should an application for that information be made under FOIA 2000 it is likely that the information would be exempt from disclosure and the public interest lie in favour of withholding. However, nothing in this paragraph shall prevent the individual Partner Organisations from exercising its obligations and responsibilities under FOIA 2000 as it sees fit.

The Subject Access Requests will be handled by the GP Practice where the patient is registered. If the patient requires information regarding their visit / attendance at the extended access service hub, this will be sent to the individual practice once the patient has been seen and the consultation is completed.

7. REVIEW OF DATA SHARING AGREEMENT

This agreement will be reviewed March 2019 and annually thereafter dependent on the funding of the scheme. It may be necessary to update the agreement in year. If any changes are to be made, these will be communicated to practices with new agreements for authorisation and changes will be highlighted. Where necessary, fresh approvals will be sought from the LMC, CCG and patient groups.

8. FREEDOM OF INFORMATION ACT (2000) (FOIA)

The practice may wish to upload this data sharing agreement to its practice website to inform the patients and public of the data sharing regarding GP hubs. Information regarding the details of this agreement may be requested by members of the public under the Freedom of Information Act 2000. Any requests made to GP Practices should be forwarded to the Primary Care Teams at the associated Clinical Commissioning Groups. The CCG's will then contact Midlands and Lancashire Commissioning Support Unit FOI Team. mlcsu.foi@nhs.net. The FOI team will assist the CCGs in responding to any FOI requests. Closure/termination of agreement

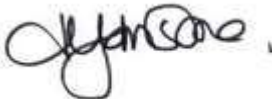
9. CLOSURE/TERMINATION OF AGREEMENT

Any of the parties can opt out of this sharing agreement at any time but must provide a notice period of not less than 30 days. This must be communicated in writing to the Head of Primary Care Commissioning in the Primary Care Team at the associated Clinical Commissioning Groups. It is the responsibility of the practice opting out to communicate this to all the partners to the data sharing agreement and inform the EMIS provider to stop the access to the practice data from the hub. If a practice does decide to opt of the data sharing agreement, then it is the responsibility of the GP Practice to communicate to patients that they can no longer access the urgent care hub for appointments due to this termination of sharing information.

10. SIGNATORIES

Each partner should identify who is the most appropriate post holder within their agency to sign the agreement having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their organisation to the indemnity. In most cases it will be the organisation's Caldicott Guardian who will be signatory to data sharing agreements. It is the responsibility of the individuals identified at 3.2 to ensure that copies of the agreement are made available as necessary to ensure adherence to the agreement.

Signatories:

Name	Heather Johnstone	Name	Dr Steve Fawcett
Role	Caldicott Guardian	Role	Caldicott Guardian
Organisation	NHS South East Staffordshire and Seisdon Peninsula CCG	Organisation	NHS Stoke on Trent CCG
Signature		Signature	
Date	24.08.2018	Date	24.08.2018

Name		Name	
Role		Role	
Organisation		Organisation	
Signature		Signature	
Date		Date	

Appendix A – Parties to the Agreement

North Staffordshire GP Federation – The list below shows the practices that the Extended Access Service Hub is providing the extended access service on behalf of:

CCG	Practice Code	GP Practice Name
Stoke on Trent	M83004	Mayfield Surgery
North Staffs	M83005	Heathcote Street Surgery
North Staffs	M83007	The Village Surgery
North Staffs	M83011	Werrington Village Surgery
North Staffs	M83012	Leek Health Centre
Stoke on Trent	M83014	Trent Vale Medical Practice
North Staffs	M83015	Moss Lane Surgery
North Staffs	M83017	Ashley Surgery
Stoke on Trent	M83021	Furlong Medical Centre
North Staffs	M83023	Kidsgrove Medical Centre (Dr Harbidge)
North Staffs	M83025	Miller Street Surgery
Stoke on Trent	M83028	Glebedale Medical Centre
North Staffs	M83034	Silverdale Village Surgery
Stoke on Trent	M83038	Orchard Surgery
North Staffs	M83046	Biddulph Valley
Stoke on Trent	M83047	Meir Park and Weston Coyney Medical Practice
North Staffs	M83054	Audley Health Centre
North Staffs	M83056	Wolstanton Medical Centre
Stoke on Trent	M83061	Millrise Medical Practice
Stoke on Trent	M83066	Hartshill Medical Centre
North Staffs	M83067	Lyme Valley Medical Centre
Stoke on Trent	M83068	Belgrave Medical Centre
North Staffs	M83071	Park Medical Centre
Stoke on Trent	M83075	Norfolk Street Surgery
Stoke on Trent	M83076	Harley Street Medical Centre
North Staffs	M83079	Moorland Medical Centre
Stoke on Trent	M83082	Haymarket Health Centre
North Staffs	M83084	Dr Robinson's and Partners
North Staffs	M83089	Biddulph Doctors
Stoke on Trent	M83090	Dunrobin Street Medical Centre
Stoke on Trent	M83094	Brook Medical Centre
North Staffs	M83096	Tardis Surgery
Stoke on Trent	M83100	Dr Miles and Partner
Stoke on Trent	M83102	Potteries Medical Centre
North Staffs	M83103	Allen Street
North Staffs	M83108	Well Street Surgery
North Staffs	M83121	Tean Surgery
North Staffs	M83122	Waterhouses Surgery
Stoke on Trent	M83123	Birches Head Medical Centre
Stoke on Trent	M83126	Longton Hall Surgery
Stoke on Trent	M83127	Cobridge Surgery
Stoke on Trent	M83128	Merton Street Surgery
Stoke on Trent	M83134	Foden Street Surgery
Stoke on Trent	M83138	Drs Shah and Talpur

North Staffs	M83140	Higherland Surgery
North Staffs	M83141	Kingsbridge Medical Practice
Stoke on Trent	M83143	Goldenhill Medical Centre
Stoke on Trent	M83146	Moorcroft Medical Centre
Stoke on Trent	M83601	Brinsley Avenue Practice
Stoke on Trent	M83619	Drs Rees and Lefroy
Stoke on Trent	M83623	Snowhill Medical Centre
Stoke on Trent	M83624	Cambridge House Surgery
Stoke on Trent	M83625	Hanley Health Centre
Stoke on Trent	M83627	Apsley Surgery
Stoke on Trent	M83632	Trinity Medical Centre
North Staffs	M83640	Alton Surgery
Stoke on Trent	M83650	Tunstall Primary Care
Stoke on Trent	M83661	Adderley Green Surgery
North Staffs	M83665	RJ Mitchell
North Staffs	M83670	Keele University Practice
Stoke on Trent	M83682	Lucie Wedgwood Medical Centre
North Staffs	M83691	Betley Surgery
North Staffs	M83697	Milehouse Medical Practice
Stoke on Trent	M83700	Five Towns Surgery
North Staffs	M83701	Talke Clinic
Stoke on Trent	M83709	Baddeley Green Surgery
Stoke on Trent	M83711	Trentham Mews Medical Centre
Stoke on Trent	M83712	Dr A K Sinha
Stoke on Trent	M83713	Dr Borse and Partner
Stoke on Trent	M83714	Dr S B Kulkarni
North Staffs	M83723	Loomer Road Surgery
Stoke on Trent	M83725	Dr Mir
Stoke on Trent	Y00592	Moss Green Surgery
Stoke on Trent	Y02521	Willowbank Surgery
North Staffs	Y02570	Midway Medical Centre
Stoke on Trent	Y02867	Middleport Medical Centre

East Staffordshire Primary Care Partnership – The list below shows the practices that the Extended Access Service Hub is providing the extended access service on behalf of:

CCG	Practice Code	GP Practice Name
East Staffs	C81018	Dover River Practice
East Staffs	M83010	Gordon Street (The Surgery)
East Staffs	M83013	Yoxall Health Centre
East Staffs	M83026	Carlton Group Practice
East Staffs	M83027	Trent Meadows
East Staffs	M83035	Alrewas Surgery
East Staffs	M83037	The Tutbury Practice
East Staffs	M83042	Bridge Surgery
East Staffs	M83051	Wetmore Road Surgery
East Staffs	M83059	Abbots Bromley Surgery
East Staffs	M83065	Barton Family Practice
East Staffs	M83073	Stapenhill Medical Centre
East Staffs	M83074	Balance Street Practice
East Staffs	M83641	Mill View Surgery

East Staffs	M83680	Northgate Surgery
East Staffs	M83681	All Saints Surgery
East Staffs	M83718	Peel Croft Surgery
East Staffs	Y00078	Winhill Medical Centre

The Mercian GP Network – The list below shows the practices within South East Staffs and Seisdon Peninsula (SES&SP) that the Extended Access Service Hub is providing the extended access service on behalf of:

CCG	Practice Code	GP Practice Name
SES&SP	M83032	Aldergate Medical Practice
SES&SP	M83062	Laurel House Surgery
SES&SP	M83088	Hollies Medical Centre
SES&SP	M83110	Heathview Medical Practice
SES&SP	M83111	Riverside Surgery
SES&SP	M83113	Dr Khare – Stonydelph Medical Centre
SES&SP	M83117	Crown Medical Practice
SES&SP	M83148	Peel Medical Practice
SES&SP	M83693	Tri Links Medical Practice
SES&SP	M83705	Trinity Medical Centre
SES&SP	M83706	Dr Rajput – Stonydelph Medical Centre

GP First – The list below shows the practices within Stafford and Surrounds (SAS), South East Staffs and Seisdon Peninsula (SES&SP) and Cannock Chase that the Extended Access Service Hub is providing the extended access service on behalf of:

CCG	Practice Code	GP Practice Name
SAS	M83009	Brewood Medical Practice
SES&SP	M83018	Gravel Hill Surgery
SAS	M83020	Cumberland House Surgery
SAS	M83024	Castlefields Surgery
SES&SP	M83031	Russell House
SAS	M83036	Rising Brook Surgery
SES&SP	M83041	Moss Grove Surgery Kinver
SAS	M83044	Stafford Health & Wellbeing Centre
SAS	M83045	Penkridge Medical Practice
SAS	M83049	Holmcroft Surgery
SAS	M83050	Wolverhampton Road Surgery
SAS	M83052	Weeping Cross Health Centre
SAS	M83057	Mill Bank Surgery
SAS	M83069	Mansion House Surgery
SAS	M83070	Gnosall Surgery
SAS	M83092	The Crown Surgery
SES&SP	M83093	Dale Medical Practice
SES&SP	M83097	Bilbrook Medical Centre
SES&SP	M83125	Claverley (The Surgery)
SES&SP	M83132	Lakeside Medical Centre
SES&SP	M83668	Tamar Medical Centre
Cannock Chase	M83703	Brereton Surgery
SES&SP	M83715	Featherstone Family Health Centre
Cannock Chase	M83738	Aelfgar Surgery
Cannock Chase	Y02354	Sandy Lane Surgery

Cannock Chase Clinical Alliance – The list below shows the practices within Stafford and Surrounds (SAS) and Cannock Chase that the Extended Access Service Hub is providing the extended access service on behalf of:

CCG	Practice Code	GP Practice Name
Cannock Chase	M83001	Horsefair Practice
Cannock Chase	M83016	High Street Surgery
SAS	M83022	Hazeldene House Surgery
Cannock Chase	M83033	Dr Chandra – Hednesford Valley Health Centre
Cannock Chase	M83048	The Nile Practice
Cannock Chase	M83063	Norton Canes Health Centre
Cannock Chase	M83107	Alderwood Medical Practice
Cannock Chase	M83109	Dr Singh and Dr Manickam
Cannock Chase	M83129	Heath Hayes Health Centre
Cannock Chase	M83130	The Red Lion Surgery
Cannock Chase	M83139	Moss Street Surgery
Cannock Chase	M83608	The Quinton Practice
Cannock Chase	M83616	Dr I Rasib
Cannock Chase	M83637	Chadsmoor Medical Practice
Cannock Chase	M83638	The Colliery Practice
Cannock Chase	M83698	Southfield Way Surgery
Cannock Chase	M83717	Norton Canes Surgery
Cannock Chase	M83719	Rawnsley Road Surgery
Cannock Chase	M83722	Dr Murugan
Cannock Chase	M83727	Norton Canes Practice
Cannock Chase	Y02594	Essington Medical Centre

Lichfield and Burntwood GP Network – The list below shows the practices within South East Staffs and Seisdon Peninsula (SES&SP) that the Extended Access Service Hub is providing the extended access service on behalf of:

CCG	Practice Code	GP Practice Name
SES&SP	M83006	The Westgate Practice
SES&SP	M83030	Langton Medical Group
SES&SP	M83072	Salters Meadow Health Centre
SES&SP	M83115	Boney Hay Surgery
SES&SP	M83617	Darwin Medical Practice
SES&SP	Y02414	Burntwood Health & Wellbeing Centre

Appendix B – EMIS Remote Consultations Configuration Request



EMIS WEB REMOTE CONSULTATIONS CONFIGURATION REQUEST

Remote Consultations enables you to add appointments into other Enterprise Organisations' Appointment Books and cancel any appointments you have booked.

This document is intended to provide us with the appropriate information in order to configure Remote Consultations for all parties listed within the appointment receiving organisation and appointment booking organisation tables. We will be forwarding information onto the main contact for each of the respective organisations, providing an overview of the Remote Consultations sharing details.

If any of the organisations to be included in this request have previously been configured for a 'Remote Consultation Agreement', the organisation will already be identified as an 'Enterprise Customer' within their EMIS Web system and we would ask that this is also confirmed when completing the organisation details section of this form.

This document is **not** a sharing agreement, you must contact your local information governance officer in order to discuss your sharing requirements and arrange for any local respective sharing agreement to be drawn up between all parties.

This document must be completed electronically and returned in word format from an email address that has been verified by us. When complete, please email the form to:

- If this has been ordered as part of a Clinical Service, cfclinicalsystems@emishealth.com
- If this has been ordered separately, cfdatasharing@emishealth.com.

8. REQUESTOR DETAILS

These are your details and signoff for the organisation submitting the configuration request.

This organisation will receive the implementation Solutions Optimisation Day and Training Day.

(Note: if you want to be included in this sharing agreement you will need to add your organisation details to the 'sharing organisation details' table below)

Organisation/Trust Name	
Address	
Main Contact (Requesting Organisation)	Name:
	Job title:
	Telephone:
	Email:
Customer Number	
Date	

9. REMOTE CONSULTATIONS SHARING DETAILS

Provide details as to what information is required to be shared by all the sharing organisations.

Agreement Name	
Agreement Short Name	
Detailed Agreement Description (Must detail WHAT and WHY the data is to be shared)	

10. ORGANISATION DETAILS

Please populate the table with all organisations wishing to allow/receive and/or book appointments, if you are making a change to an existing agreement please highlight the changes.

Please ensure that organisations also follow the guidance from EMIS Health on the Firewall Settings by viewing the IF2092 EMIS Web Third Party Network Access Advisory document.

Note: *If an organisation listed on this request is already configured as an Enterprise Customer, i.e. is included as part of another Remote Consultation Configuration Agreement, please advise in the table below*

Customer Number	NACS Code	Organisation Name	Email address (main contact)	Are you an existing Enterprise Customer



ASSOCIATED DOCUMENTATION

IF2092 EMIS Web Third Party Network Access Advisory

No part of this document may be sold, hired, reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording and information storage and retrieval systems for any other purpose than the purchaser's use

without the express written permission of EMIS Health.

Every effort is made to ensure that your EMIS Health documentation is up to date, but our commitment to constantly improve our software and systems means that there may have been changes since this document was produced.

Web: www.emishealth.com

Appendix C – Medical Interoperability Gateway (MIG) Data Sharing Agreement



healthcare gateway

Connecting you to real-time patient
data from any care setting

Medical Interoperability Gateway (MIG) Detailed Care Record Service (DCR) Data Sharing Information

Purpose of this document

The purpose of this document is to provide Healthcare Gateway Limited (HGL) customers and potential customers an overview of the information required by HGL in order to enable data sharing between different Health Organisations.

Introduction

Prior to the technical activation of the MIG in any given locality, Healthcare Gateway Limited require evidence of the signed data provider sharing agreements. These sharing agreements will have been defined and agreed by the data controller e.g. GPs to determine which consuming organisations have access to which elements of the clinical record.

Information required

As a minimum the following information is required by Healthcare Gateway Limited before enabling data sharing between a provider (sharer) and consuming (viewing) organisation

- **Details of the organisation sharing the data (name of organisation, data controller, NACS/ODS code, supplier reference code)**
- **What information is being shared and for what purpose?**
NB: all practices must agree to share the same level of data with any one organisation. If associated free text is to be included for the DCR v2 service it should be stipulated.
- **Details of the Organisation who will be viewing the data (name of organisation, data controller, NACS/ODS code, supplier reference code)**

The agreement must be signed by the data controller of the data from each sharing organisation e.g. the GP practice

Information sharing agreement

HGL have produced an example information sharing agreement that can be used to ensure the above items are covered sufficiently, please see appendix A of this document

It should be noted whilst this agreement cover the minimum information required by HGL to enable data sharing, HGL strongly recommend that customers liaise with their Information Governance Department and Caldecott Guardian to discuss the information governance requirements for projects involving the sharing of patient data.

Appendix A – example MIG DCR information sharing agreement

Agreement name	Information Sharing Agreement between [<i>Organisation name</i>] and [<i>Organisation name</i>]
Purpose of the Sharing Agreement	
<p>The purpose of this Information Sharing Agreement (ISA) is to provide integration of the MIG Detailed Care Record (DCR) service from [<i>Organisation name</i>] to the [<i>Organisation name</i>]</p> <p>Healthcare Gateway will provide the MIG technology and hosting infrastructure to support the interoperability between provider (sharing) organisations and consumer (viewing) organisations</p>	

We [*organisation name*] agree to share the following patient information via MIG.

MIG Detailed Care Record
Patient Demographics
Summary, including Current Problems, Current Medication, Allergies, and Recent Tests
Problem view
Diagnosis View
Medication including Current, Past and Issues
Risks and Warnings
Procedures
Investigations
Examination (Blood Pressure Only)
Events consisting of Encounters, Admissions and Referrals

Specialist Dataset
[<i>Enter name and reference as applicable</i>]

Provider (sharing) organisation

Practice/organisation name	
Address	
NACS/ODS code	
Supplier Reference Number	
Name and role	

Signed (on behalf of the practice/organisation)	
Date	

Consumer (viewing) organisation

Organisation	
Address	
NACS/ODS code	
Name and role	
Signed (on behalf of the organisation)	
Date	

1. Purpose of agreement

This agreement has been developed to document the flow of information between the named organisations to enable monitoring of patients being cared for and to provide accurate data for patient service delivery. Through this agreement all parties agree to ensure that staff are made aware of their responsibilities and comply with the law and demonstrate compliance with the Data Protection Legislation, Department of Health Code of Confidentiality and the Health and Social Care (Safety & Quality) Act 2015.

2. Scope of agreement

The agreement covers the flow of information between the named organisations as to assist service delivery. This agreement is limited to information shared between the parties that are defined in this agreement and does not include any information sharing outside of the scope of this agreement

3. Approval

This agreement can only be signed by the organisation's Caldicott Guardian or an appropriate senior officer, nominated by an organisations' Caldicott Guardian/Information Governance Lead.

4. Monitoring of agreement

Each organisation signed up to this agreement is responsible for ensuring full compliance of all staff within their organisation to the terms and conditions of this agreement. Any identified areas of non-compliance must be forwarded to the Nominated Senior Professional for resolution.

Note: Once the information is made available to the consuming system HGL shall not be held liable for the Data Recipient's use and governance of such information.

5. Access to patient information

Clinical and personal details will only be available to any person who is involved with the care of the individual on a need-to-know basis. Professionals must be able to justify fully the reasons for their obtaining any particular detail about an individual. Before anyone can view the shared record there must be a legitimate relationship with the patient and permission from the patient to view the shared record or stated that there was an emergency override

Associated documentation

HGQM009 Healthcare Gateway MIG Content Model Read Code Mappings to Record Elements

EXT584 TPP Implementation of the MIG DCRV1 Content Model

Disclaimer

No part of this document may be sold, hired, reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording and information storage and retrieval systems for any other purpose than the purchaser's use without the express written permission of Healthcare Gateway.

Contact information

Healthcare Gateway, Unit 3 Rawdon Park, off Green Lane, Rawdon, Leeds, LS19 7BA

enquiries@healthcaregateway.co.uk

www.healthcaregateway.co.uk

0845 601 2642