NHS
Manchester
Clinical Commissioning Group

GP INFORMATION DATA SHARING CONTRACT

Between the Data Controller:-

Insert GP Practice Code, Practice Name and Address

And the Data Processor

Manchester Clinical Commissioning Group
Parkway Business Centre, Parkway Three, Princess Road, Manchester, M14 7LU

Purpose / Title:
The purpose of this agreement is for GP Practices to share information to support the Greater Manchester Care Record (MCR) and the delivery of the integrated health and social care programme

Start Date: 02/04/2018 **Review Date:** 31/03/22 *

*This agreement will be reviewed annually by the Information Strategy and Advisory Group (ISAG) but is valid until the review date above.

Title:	GP Information Data Sharing Contract
Version:	V5.5
Date:	02/04/18
To be Reviewed:	31/03/22

GP INFORMATION DATA SHARING CONTRACT

1. Introduction

This contract forms an agreement between the parties listed above and seeks to:

- Set out the responsibilities of the parties in relation to the information provided by GP Practices
- Outline security and confidentiality requirements on the CCG (The Data Processor)
- Sets out the purpose for sharing, the agreed uses of the information (see schedule 1), the data to be shared, the legal basis and the method of data transfer

This contract covers the sharing of information held within GP Practice clinical systems for the purposes listed in schedule 1 and takes into account the legal requirements and government guidelines governing the sharing of patient confidential data.

2. GP Practice Responsibilities (Data Controller)

Under the terms of the current Data Protection Act (DPA) 2018 and the General Data Protection Regulations (GDPR), GP Practices are the data controllers of the information held within their clinical systems.

As such the GP Practice is the Data Controller for the information shared as part of this contract and has a responsibility for ensuring the sharing complies with the DPA and GDPR and is fair and lawful. The GDPR principles are listed in Appendix 2.

Fair Processing

GDPR requires the fair processing of personal data in a transparent manner. This means patients should be generally aware of the information sharing covered by this contract, why the data is being shared and for what purpose.

GP Practices must use a range of measures such as a privacy notices on their website, patient leaflets and posters so patients can access it if they want to. This approach is acceptable where the data sharing is something people are likely to expect or be aware of already, and to which people are unlikely to object.

Lawful Processing

Fair and lawful processing requires adherence to the common law duty of confidentiality and the GDPR Principles (as summarised at Appendix 2).

The GDPR sets out conditions for lawful processing of personal data (Article 6) and further conditions for processing special categories of personal data (Article 9). As personal data concerning health is one of the special categories, organisations that process such data must be able to demonstrate that they have met a condition in both Article 6 and Article 9.

The revised Data Protection Act 2018 will make further provision in respect of the lawful bases for processing special categories of personal data.

The data sharing set out in this agreement satisfies the following conditions:-

Article 6(1)(e): the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

Article 9(2)(h): The special category condition for processing for direct care is that processing is: 'necessary for the purposes of preventative 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'.

Clinical Commissioning Group Responsibilities

The CCG is acting as a Data Processor and must process the data in accordance with the principles as set out under the terms of the GDPR.

The CCG will only use the data for the purposes specified within this contract unless instructed to do otherwise by the GP Practice. Any additional uses authorised by the GP Practice will be set out in an additional Data Sharing Agreement (DSA).

The CCG will not share the data with any organisations not listed within this contract or any subsequent data sharing agreements.

The CCG will comply with the Information Security requirements as set out in section 4 of this contract, and ensure that any further data processors with access to the information are subject to equivalent requirements.

The CCG will notify the data controller of any data breaches.

The CCG will undertake a Data Protection Impact Assessment and make this available upon request to the GP Practice to provide assurance that appropriate security controls are in place.

The CCG will have confidentiality, information security, data protection and records management policies, including individual responsibilities for handling data and will be supported by an appropriate disciplinary policy.

It is noted that should Manchester CCG (Data Processor) break this contract with the GP Practices (Data Controller) for example by using the data for purposes not stated within this contract or any data sharing agreements, then it will take on its own Data Controller responsibilities. This includes the duty under the first principle of GDPR to process, including obtaining, personal data fairly, lawfully and in a transparent manner. Where a Data Processor takes the personal data the Data Controller has entrusted it with but breaks the terms of its contract by using the data for its own purposes, it is likely to be in breach of the first principle and the Information Commissioners Office (ICO) could take enforcement action against it. In this case, the CCG will notify the ICO of the breach.

3. Information Sharing Strategy & Advisory (ISAG) Group

Schedule 1 of this document sets out the permitted uses of the information being shared as part of this contract which can be are summarised as:

- Every patient registered with a Manchester GP will automatically be enrolled onto the Manchester Care Record for the purposes of supporting direct health and social care.
- Use of the GP extract to support Risk Stratification in accordance with Section 251 of the Health and Social Care Act 2012. Arden and GEM CSU provide Risk Stratification to the MCR.
- Use of anonymised information by analytical staff to support commissioning and GM health intelligence.

The ISAG will be chaired by the Caldicott Guardian with representatives from the Local Medical Committee (LMC); Care Provider organisation's contributing to the Manchester Care Record and the CCG as the Data Processor. A member of the LMC is required to be in attendance at the ISAG to ratify any decisions put forward, if this is not possible, any decisions would need to be approved electronically by the LMC.

Any recommendations relating to the extended use of the information shared as part of this agreement will be drawn up as an annex to this agreement. All approved cases will be documented and shared to all data controllers as an annex to this agreement and together will form the overall agreement.

The CCG will only process information for the recommended purpose once the GP Practice has signed the Data Sharing Contract.

4. Information Security

The CCG (Data Processor) will process the data at all times:

- In accordance with the DPA and GDPR.
- Using appropriate technical and organisational measures to ensure the protection of the information subject to this agreement against the accidental loss or destruction of or damage to the data supplied, having regard to the specific requirements set out in this contract, the state of technological development the cost of implementing measures and the level of harm that might result from the unauthorized or unlawful processing of the data or by its loss damage or destruction.

The CCG will not transfer the data outside of the European Economic Area (EAA) or to any organisation not listed within this contract or any associated Data Sharing Contracts.

The CCG agrees to:

- Store and process the data securely;
- Maintain good information governance standards and practices, and achieving compliance with the new Data Security and Protection Toolkit.
- Ensure reasonable background checks to ensure the reliability of all employees who have access to the data;
- Ensure appropriate confidentiality clauses are included in its employment contracts;
- Ensure access to the data is managed, auditable and restricted to those needing access to the data. Access to the Manchester Care Record will be managed by:

    - **User sponsorship and registration process**
    - **Induction and training processes for users**
    - **Legitimate relationship access** – staff are associated with one or more GP practices on the system
    - **Roles-based access** – access can be controlled to a specific document, data element or type depending on their service role.
    - **Function access** based on user role - controls over the functions to create, edit or read-only elements of the record.
    - **Consent to access** – users are required to record, via the screen-prompts, the legitimate basis for accessing the record.
    - **Access audit-trail** – full recorded audit trail of access and views of the record.

Users of the data are required to comply with the Data Protection Act 2018/GDPR and the Common Law Duty of Confidentiality together with all related and relevant legislation and Department of Health directives relating to data sharing (See Appendix 1).

5. Audit

The GP Practices have the right to request an audit of the data processors use of the data and security controls.

6. Indemnity

When using the Manchester Care Record (MCR) the CCG shall indemnify the GP Practice in full for any civil penalty imposed by the Information Commissioner or (civil) court action by way of a civil monetary penalty under Article 83 of the GDPR, if it is incurred as a result of:

The Clinical Commissioning Group (data processor) losing data.

- Following the unauthorised or unlawful use of data by the Clinical Commissioning Group or Partner organisation.
- Through the negligence of the Clinical Commissioning Group, its employees or partners.
- The Information Commissioners Office (ICO) or Court ruling later finds that the basis for sharing data was unlawful.

7. Incident Management

Both the GP Practice (data controller) and CCG (data processor) have responsibility to monitor all Information Governance related incidents that occur that may breach security and / or confidentiality of personal information.

The member of staff reporting an incident should follow their organisation's Incident Reporting Policy/Procedure. The Information Governance Lead of the reporting organisation should disseminate details about the incident to any other partner organisation that may be affected. Under Article 33 of the GDPR, Data controllers will be obliged to report certain types of IG breaches to the Information Commissioners Office "without undue delay, and where feasible, no later than 72 hours" after they first become aware of it.

Where the reporting organisation is a GP Practice (Data Controller), they should also inform the CCG (Data Processor) of the incident.

8. Restrictions on use of the information shared

All shared information, personal or otherwise, must only be used for the purpose(s) listed in schedule 1 of this agreement or an additional data sharing agreement signed by the GP Practice (Data Controller) unless otherwise required or permitted by law.

Restrictions may also apply to any further use of non-personal information, such as commercial sensitivity or prejudice to others caused by the information's release, and this should be considered when considering secondary use of non-personal information. If in doubt the Data Controller should be consulted.

9. Information Quality

The GP Practice will ensure the information to be shared is accurate and, where necessary, up to date.

If shared information is found to be inaccurate, it is the responsibility of the organisation discovering the inaccuracy to notify the GP Practice (data controller). The originating organisation will ensure that the data it holds is corrected and will notify all recipients, who will be responsible for updating the information they hold.

The CCG is responsible for applying reasonable data quality checks during the processing of the information.

10. Patient Information Rights

The GP Practice will comply with the rights of individuals under the Data Protection Act 2018/GDPR and (in respect of the information for which they are public authorities) the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

GDPR is very clear about data subjects being able to object how their data is processed. This includes the right to object to their data being used for secondary purposes.

Details of the NHS Digital National data opt-out programme can be found at: https://digital.nhs.uk/services/national-data-opt-out-programme

Patients and the public who decide they do not want their confidential patient information used for planning and research purposes will be able to set their national data opt-out choice online. NHS Digital will also provide a non-digital alternative for patients and the public who can't or don't want to use an online system. Individuals can change their mind anytime. Existing Type 2 opt-outs (the option for a patient to register with their GP, to prevent their confidential patient information leaving NHS Digital) will be converted to the new national data opt-out. Patients with type 2 opt-outs will be informed of this change individually.

NHS Digital is developing the system now. Patients and the public will be able to use the system from 25 May 2018. All health and care organisations will be required to uphold patient and public choices by March 2020. The national data opt-out will be introduced alongside the new data protection legislation.

If the new code is applied to a patient's record the CCG will not extract any data from the GP clinical system for that patient. If data has been previously extracted prior to the recording of the new code within the patient's record their inclusion will result in the supporting GP data being deleted from the Manchester Care Record. However, the actual record will remain active until an end date has been manually inputted. When a record is ended it will be archived and remain in the system (please see the Retention and Disposal section on page 8).

Schedule 1: Information Sharing Details

1. Manchester Care Record (MCR)

The MCR is a repository of Health and Social Care Data across Greater Manchester (GM).

- Manchester CCG GP Practices
- Manchester City Council
- Greater Manchester Mental Health NHS Trust
- Manchester University NHS Foundation Trust
- Pennine Acute Hospital NHS Trust
- North West Ambulance Service NHS Trust

or any subsequent Trust as a result from any the Single Hospital Programme.

A key component of the MCR is the extraction of 'read coded elements' of a patients GP record. No free text contained within the patients record will be extracted, only 'read codes' and any associated values such as a blood pressure reading.

The Manchester Care Record contains the 'Read coded elements' of a patients GP record for all patients who have not opted out.

Accessing the Manchester Care Record

A clinician can only view the 'Read coded elements' of a patient's GP record included within the Manchester Care Record in the following circumstances-

- For the purposes of direct patient care

- 9(2)(c) - in an emergency or life threatening situation where the patient is unable to consent and delay in accessing information would not be in the patient's best interests, the GP/health professional can access the record. A justification for accessing the information will be required in order to do this and will be recorded for routine monitoring. If the patient is under the age of 18 and unable to consent, the consent of someone with parental responsibility should be obtained, provided the time necessary to take this step will not adversely affect the patient

Retention and Disposal

GP Practices should retain their information in accordance with the Records Management Code of Practice for Health and Social Care (July 2016), and dispose of it securely when it is no longer needed.

Details can be found at:

https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

1. The flow of GP patient information as described within schedule 2 of this GP Information Data Sharing Contract will cease if the patient opts-out of the MCR or has died.

2. The inclusion of an end date within a patient's MCR will result in the record becoming inactive and only visible to the system administrator for a period of 2 years.

3. The NHS Records Management Code of Practice states that the minimum retention period is 8 years after death of a patient. Although there are different retention periods e.g. for mental health activity 20 years after the last contact; for children's records until their 26th birthday, the MCR is a 'read only' limited copy of each Data Controllers source data.

Therefore, on a monthly basis any records with an end date of 8 years or more will be destroyed securely along with any associated care records.

2. Dataset, frequency and method of extraction

The Table 1 summarises the information that will be shared as part of this contract and for what purposes. Table 2 describes the data flows and the method of data transfer.

Table 1

INFORMATION SHARING DETAILS FORM	
Description of Task / Purpose of Data Collection / Extraction: *(including any additional information such as - details of project / contract / service / legislation)*	The coded elements of the patients Manchester Care Record (MCR) will be extracted from the GP Practices Clinical System to support the following processes for direct patient care: • Care Planning: identifiable coded data will be made available to members of GM Integrated Care Teams. The MDTs consist of the health and social care practitioners directly involved in the patients care where a legitimate relationship exists. • Electronic Palliative Care Co-ordination System (EPaCCS): identifiable data will be made available for patients with an EPaCCS record. • Risk stratification: data will be used to risk stratify patients according to their risk of emergency admission to hospital to support case finding. Only GP Practices will be able to view identifiable information via a secure clinical Dashboard which will be provided by North of England Commissioning Support Unit. • Primary Care Clinical Dashboards: the data will be used to support case finding and management of patients with Long Term Conditions. Only GP Practices will be able to view identifiable information via a secure clinical dashboard which will be provided by Arden and GEM Commissioning Support Unit. • Health Intelligence: pseudonymised versions of the data will be created and used to support these commissioning activities such as needs assessment and service evaluation locally and across Greater Manchester (GM). Commissioning and business intelligence staff with access to this data will be prohibited from taken any steps that could lead to the identification of the patient. • Access to the MCR from the Emergency Department (ED) at GM Provider Trusts. • Access to the MCR from GM Provider Trusts.

	• Access to the MCR from Out Of Hours (OOH) providers in GM. • Access to the MCR from North West Ambulance Service (NWAS). • For the recording of Child Health Vaccinations linking to the GM child health system. • To support data sharing needs outside of the requirements listed above that have been identified and approved by the Information Sharing and Advisory Group (ISAG).
Frequency of Collection / Extraction / Access:	Daily
Description of data to be collected/extracted: (include all data items required)	The dataset that is extracted includes the following items:- NHS Number Entry Date Read Code Rubric (Read Code Description) Code Value Code Units Information covered by the following legislation is not extracted:- AIDS (Control) Act 1987, NHS (Venereal Diseases) Regulations 1974; NHS Act 1977; NHSTs & PCTs (STDs) Directions 2000, Human Fertilisation & Embryology (Disclosure of Information) Act 1992
Will patient identifiable data be needed?	Yes - NHS Number
Who will have access to data or where will the data be sent?	The data will be stored within the Greater Manchester IM&T Shared Service secure Data Centre. A subset of the data will also be sent to the Arden and GEM Commissioning Support Unit (CSU) for inclusion within their Risk Stratification tool and clinical Dashboards. GP Practices will have access to the information along with Multi-Disciplinary Team members for consenting patients. Clinical staff with a legitimate patient relationship, such as (but not limited to): ED Clinicians, Ambulance and Paramedic staff, Acute secondary care providers and Out Of Hours (OOH) providers. Analytical staff will only have access to pseudonymised information to support commissioning and health intelligence. Risk Stratification for this purpose is undertaken by Arden and GEM CSU. IT and Database Administrators will have access to the system for maintenance purposes.

Schedule 2: Information Flow Details

Table 2

Data	From	To	Method of Transfer of Information	Frequency	Purpose
NHS Number Entry Date Read Code Rubric Code Value Code Units	GP Practice	Manchester CCG Secure Data Extraction System hosted by Greater Manchester Shared Service	Data is transmitted between the GP system in the EMIS hosted environment and Secure Data Extraction System via the new secure Health and Social Care Network (HSCN). All data transactions between the GP system and the Secure Data Extraction Systems are recorded in an audit trail. Patient data can be transmitted in a variety of message formats (e.g. HL7, CSV, XML, Binary Files (PDF, XPS, DOC, DOCX, images etc)) that are encrypted using the approved Secure Sockets Layer (SSL) encryption standard. The data is stored on a server in a locked and secure data centre hosted by the Greater Manchester Shared Service.	Daily	• Manchester Care Record • Risk Stratification • Clinical Dashboards • Health and Commissioning Intelligence
NHS Number Entry Date Read Code Rubric Code Value Code Units	Manchester CCG Secure Data Extraction System hosted by Greater Manchester Shared Service	North of England Commissioning Support Unit	A subset of data will be encrypted and transferred via the new secure Health and Social Care Network (HSCN).	Monthly	• Risk Stratification • Primary Care Clinical Dashboards

Schedule 3 Signatories

Name of GP Practice			
Caldicott Guardian	**Contact Details**	**Signature**	**Date**
	Address: **Tel:** **Email:**		
Practice Manager	**Contact Details**	**Signature**	**Date**
	Address: **Tel:** **Email:**		

Clinical Commissioning Group	**Manchester Clinical Commissioning Group**		
Caldicott Guardian	**Contact Details**	**Signature**	**Date**
Manisha Kumar	**Address:** Second Floor, Parkway Business Centre, Parkway 3, Princess Rd, Manchester M14 7LU **Email:** manisha.kumar1@nhs.net		03/07/18
Information Governance Lead	**Contact Details**	**Signature**	**Date**
Chris Upton	**Address:** Second Floor, Parkway Business Centre, Parkway 3, Princess Rd, Manchester M14 7LU **Tel:** 0161 765 4368 **Email:** christopher.upton@nhs.net		27/06/2018

APPENDIX 1 - LEGAL FRAMEWORK

All agencies are aware of the requisite legislation. This guidance does not attempt to restate our legal obligations, but recognises that we must comply with the following legislation and directives:

- Access to Medical Reports Act 1988.
- Access to Health Records Act 1990.
- The Health and Social Care Act (Safety and Quality) 2015
- The Common Law Duty of Confidentiality.
- The NHS Act 2006.
- Carers (Recognition and Services) Act 1995.
- Children's Act 1989.
- Computer Misuse Act 1990.
- Crime and Disorder Act 1998.
- Criminal Justice Act 1967
- Carers and Disabled Children Act (2000)
- Care Standards Act 2000
- Data Protection Act 2018
- General Data Protection Regulations 2016
- Domestic Violence Crime and Victims Act 2004
- Family Law Reform Act 1969.
- Family Law Act 1996
- Freedom of Information Act 2000.
- Fraud Act 2006
- Health and Social Care Act 2012
- Human Rights Act 1998.
- Mental Health Act 1983.
- Mental Capacity Act 2005
- NHS and Community Care Act 1990.
- Police and Criminal Evidence Act 1970
- Protection from Harassment Act 1997
- Public Order Act 1986
- Public Health Act 1936 and Public Health Act 1961
- Sexual Offences Act 2003
- Power of Attorney Act 1971
- Public Interest Disclosure Act 1998

Not limited to but extended to other legislations as deemed relevant.

APPENDIX 2 – PRINCIPLES OF THE GENERAL DATA PROTECTION REGULATIONS & CALDICOTT PRINCIPLES

Under the GDPR, the Data Protection Principles set out the main responsibilities for GP practices and information sharing partner organisations, these are:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and, where necessary, kept up to date;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. processed in a manner that ensures appropriate security of the personal data.

The most significant principle is the first principle which states that personal data shall be processed fairly and lawfully and shall not be processed unless at least one Article 6 condition and in the case of special category data, at least one Article 9 condition must be met.

When relying on Articles 6(1)(e) and 9(2)(h) to share data for the provision of direct care, consent under GDPR is not needed. In addition to GDPR, GP Practices must also satisfy the common law duty of confidentiality so that they can continue to rely on implied consent to share confidential health data for the provision of direct care.

The GP Practice and information sharing partner must also comply with the 7 Caldicott Principles:

Principle 1 - Justify the purpose(s) for using confidential information

Principle 2 - Only use it when absolutely necessary

Principle 3 - Use the minimum that is required

Principle 4 - Access should be on a strict need-to-know basis

Principle 5 - Everyone must understand his or her responsibilities

Principle 6 - Understand and comply with the law

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality