Information Sharing Agreement

Table of Contents

Document Control

Document Details:

Title:	*My Care Record* – Information Sharing Agreement (ISA)
Status:	Final
Version:	Version 11 created from Version 10
Document Reference:	MCR_ISA_v11
Date of Issue:	1st September 2022
Reviewed:	Information Sharing Agreement (ISA) will be reviewed to meet legislative changes or every 6 months whichever is sooner
Document Owner:	EoE IG Working Group

Revision History:

Date:	Description of Change
31-07-2019	Creation of Suffolk and North East Essex STP MCR ISA using Version 6 of MCR ISA (Draft)
16-08-2019	Incorporated approved comments from IG Delivery Group and CIAG
19-08-2019	West Essex approved
29-08-2019	Amended Logo's to include Suffolk CC and Essex CC
30-08-2019	Amendments from DPO Suffolk GP Fed
23-09-2019	Confirmation of agreement start date and email address for ISA returns
13-02-2020	Version updated to be housed online and relevant to all regions. Removal of council logos. Removal of list of organisations, replaced with instructions to view the *My Care Record* website.
01/07/2020	Reviewed by BLMK ICS IG Manager in anticipation of MCR deployment. Reviewed alongside existing BLMK high level ISA and relevant content from this document transferred to this draft version.
29/06/2020	Reviewed by M&SE IG Group
03/07/2020	Reviewed and Approved by MCR Expert Oversight Group IG members
17/03/2021	Version 8 reviewed following requested amendments from ECC
28/07/2021	Version 9 reviewed and amended following requested amendments from ECC
14.07.2022	Version 10 reviewed and amended
22/08/2022	Version 11 Approved by IGWG

Document Reviewed and Approved by:

Job Title/Review Group	Organisation	Approved
ShCR IG Working Group (IG Lead/IG Group Chair from each of	East of England Region	25/07/2022

6 ICS's)		
ICS IG Groups	East of England Region	19/08/2022
EoE IG Working Group (IG Leads from each of 6 ICS's)	East of England Region	22/08/2022

Summary Sheet

Title of Agreement	*My Care Record* – Information Sharing Agreement (ISA)
Purpose	*My Care Record* provides health and care professionals with electronic access to records by participating partner (Appendix A) organisations using new and existing secure computer systems for the purpose as detailed in Table 1. All partner organisations to this Agreement, will adopt the lawful basis for processing under current UK data protection legislation and related standards, guidelines and policies.
Partner Organisations	See Appendix A
Date Agreement comes into force	1st September 2022
Review	Will be reviewed at least every six months
Agreement review	Information Sharing Agreement (ISA) will be reviewed to meet legislative changes or every six months, whichever is soonest

Introduction

Health and care organisations have taken great strides in bringing together health and care services to improve the experience for individuals.

As part of this work, we want to ensure that health and care professionals directly involved in a person's care have access to the most up-to-date information about them.

My Care Record facilitates the lawful sharing between health and care professionals through access to records by participating partners (Appendix A) using new and existing secure systems. *My Care Record* is not an information system in itself but is an approach to information sharing.

This Agreement defines the overarching principles, requirements and controls for the secure and safe sharing of 'personal' and 'special category' data for the purpose of delivering joined-up integrated care.

In conjunction with this agreement, and in line with the IG Framework for Integrated Health & Care, partner organisations will complete a DPIA and, where necessary, enter into a *joint controller agreement*. The joint controller agreement will clearly identify which partner organisations are party to the agreement and will define specific responsibilities that the partner organisations have in accordance with UK data protection legislation.

To remove ambiguity and ensure understanding, definitions tables and DPA/UKGDPR Principles can be found at Appendix B and C of this document.

There is a requirement for this ISA to be signed and the signatory page can be found at Appendix D.

My Care Record will enable the exchange of information between each partner organisation to this Agreement in this way.

Further information can be found at: http://www.mycarerecord.org.uk/

Objectives

The objectives of this Agreement are to:

- facilitate and ensure effective access to an individual's information across relevant health and care agencies;
- enable the provision of fully integrated care to individuals whilst complying with all relevant legislation;
- provide seamless access to health and care records by health & care professionals who are involved in the individual's direct pathway of care;

- evidence the commitment of the named partner organisation to share personal information in a responsible, fair and lawful manner;
- set out the requirements which each partner organisation agrees to comply with whenever they access personal information in accordance with this Agreement;
- provide individuals with the confidence that their information is secure and viewed only by those with a legitimate justification and purpose to do so.

Table 1: Purpose of ISA	
Purpose	UK GDPR Legal Basis
Processing of personal and special category information to be acquired from and accessed across participating health and care organisations in support of *(a) direct care* by participating partner organisations and/or *(b)* Performance of the public body's adult and/or (where applicable) child social care related statutory and public law duties and powers	Personal Information Article 6(1) d - Vital interests Article 6(1) e - Exercise of official authority Special Category Information Article 9(2) h - Health or social care provision For the purposes of safeguarding children and vulnerable adults Article 9(2) b may apply
When personal and special category information is shared, the requirements of the Common law duty of confidentiality and other relevant legislation must also be considered.	

Information to be accessed

Personal information will be made available for health and care professionals from each partner organisation to view. This includes, but is not exclusive to:

- Name, address, NHS number and phone number
- Medical Conditions
- Treatment provided and contact the individual has had with the organisation
- Care Plans
- Emergency department treatment
- Discharge Summaries
- Medication Reviews
- Medical Reports
- Care and Support plans
- Care plans reviews - adult social care assessments
- Results of investigations, such as x-rays, scans, and laboratory tests

Each partner decides on the personal information that is shared with partner organisations. Details of the information that partner organisations share can be found within the collated *data flow documents/information sharing gateway.*

Where Partner organisations processing information within a shard care record as part of this agreement have decided that they will be Joint Data Controllers for the information they share/access there must be a Joint Controller Agreement in place to determine the responsibilities of each Controller

All partners are subject to a number of legal obligations to ensure that the processing of personal information remains lawful. This includes, but is not limited to the following legislation, standard, statutory and non-statutory guidance.

- UK General Data Protection Regulation (UKGDPR) (ensure article 6 and 9 are met) and the UK Data Protection Act (DPA) 2018
- Common Law Duty of Confidentiality
- Freedom of Information Act 2000
- Human Rights Act 1998 (Article 8)
- Mental Health Act 1983
- Mental Health Act 2007
- Mental Capacity Act 2005
- GMC Guidance on Confidentiality 2017
- NHS Digital Code of Practice on Confidential Information 2014
- HSCIC Guide to Confidentiality 2013
- Information Governance/Caldicott 2 Review: To Share or Not to Share
- Records Management Code of Practice for Health and Social Care 2021
- Health and Social Care Act 2022
- Health & Social Care (Quality and Safety) Act 2015
- Care Act 2014
- Care and Support Statutory Guidance
- NHS England Safe Haven Procedure
- NHS Constitution for England
- Information Security Management: Code of Practice
- ICO Data Sharing Code of Practice
- ICO Privacy Notices, Transparency and Control Code of Practice
- Data Security & Protection Toolkit (DSPT)
- Health and Social Care (National Data Guardian) Act 2018
- Health Service (Control of Patient Information Regulations (2002)
- Coronavirus Act 2020
- Public Health (Control of Disease) Act 1984
- Children Act 1989
- Security of Network & Information Systems Regulations

Principles

Each partner agrees:

- personal information shared under this agreement should only be processed for the agreed purpose
- Only clinical and social care practitioners and necessary support staff who have a legitimate relationship with the individual, shall have access to personal information about that person for the agreed purpose;
- that the duty to share information can be as important as the duty to protect individual confidentiality - a principle recommendation of the **Caldicott 2**

review of Information Governance across the Health and Social Care sectors;

- access and use of any personal information will comply fully with the requirements of data protection legislation, all other relevant associated legislation, and will follow best practice guidance issued by the Information Commissioner's Office;
- to remain the Data Controller for the information that is stored within their own Source Systems;
- to be responsible for its own compliance with the Data Protection legislation, and all relevant associated legislation, including ensuring that it has appropriate local policy and process frameworks in place to underpin best practice, safeguard personal information and protect the legal rights of *Data Subjects*;
- to undertake local Data Protection Impact Assessments where these are identified as necessary, and comply with the requirements set out in the *My Care Record* DPIA;
- to ensure security measures that ensures safe sharing are in place, so that security cannot be used as a reason for failing to share information when there is a lawful basis to share it;
- that any partner organisation may withdraw from this agreement on giving written notice to the other partners. Any information obtained whilst the organisation was partner to this agreement remains subject to the terms of the agreement and data protection legislation duties and responsibilities.
- that they will inform patients and service users about how their confidential information is used – Caldicott Principle 8 December 2020

This Agreement evidences the commitment of the named partner organisation to share information and personal information in a responsible, fair, lawful and transparent manner for the agreed purposes.

This Agreement does not constitute an overarching permission for the broad, comprehensive or unchallenged sharing of personal information for the agreed purpose.

Not all organisations will be sharing everything, information being shared would be determined by the organisation and the systems they use for the agreed purpose.

When a controller discloses personal information to another controller, each has full data protection responsibility.

Requirements

For purposes of public trust in safe and appropriate sharing of information for the agreed purpose, each partner undertakes to:

- register with the ICO and keep their registration up to date;
- not knowingly or negligently process personal information in such a way that it

places any party in breach, or potential breach, of the data protection legislation, and all other relevant associated legislation;

- implement the principles and duties outlined in the "Caldicott 2" Information Governance Review; The Care Act 2014, The Health and Social Care (Safety and Quality) Act 2015 co-operating in the exercise of functions related to health and care provision;
- ensure that 'fair processing information' has been readily made available to individuals in respect of *My Care Record*;
- only process information for the agreed purpose;
- only disclose shared information where there is a clear legal or regulatory gateway for disclosure, if no clear basis exists then partner organisation who provided the information should be consulted before release;
- notify relevant signatories in a timely manner to facilitate statutory reporting within 72 hours where a breach/incident occurs relating to data shared under this agreement;
- ensure that only health and care professionals, appropriate support staff or those with an appropriate obligation of secrecy (pursuant to Article 9(2)(h)) have access to personal information;
- implement appropriate technical and organisational measures against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information;
- put in place policies, procedures and controls that ensure full compliance with the legal requirements and obligations for sharing information;
- ensure that all staff receive role-specific data protection training annually;
- where possible, partner organisations systems should facilitate role-based access and control;
- annually self-assess and complete all mandatory assertions against the Data Security and Protection Toolkit (DSPT) and adhere to robust information governance management and accountability arrangements, including effective security event reporting and management;
- Establish effective mechanisms to ensure that personal data is only processed overseas in accordance with NHS and data protection legislation;
- facilitate the exercise of all applicable data subject rights requests under Article 15 to 22 of the UKGDPR;
- public authorities or bodies within this Agreement must appoint a Data Protection Officer (DPO), who is responsible for ensuring that data processing activities, protocols, records and structures conform to the current data protection laws;
- be individually responsible for the information that is held within their source systems where they are controller within their own right and there is no element on joint control with other partner organisations;
- be responsible for deciding what personal information will be shared from their source system to support joined up care;
- include in joint controller agreement or other data flow documentation transfer / exchange, access, storage, retention and disposal arrangements

which are appropriate to the personal information being shared between partner organisations;

- If a GP practice has agreed to allow partner organisations to view the primary care record in full, the individual (or their representative), unless clinically inappropriate, will be informed in advance and offered the opportunity to object at any point. This is in line with good practice and the common law duty of confidence. Addendum 1 gives guidance how this could be assessed, communicated and recorded.

Data quality

Each Data Controller will follow their current data quality processes, should any of the information shared be found to be inaccurate by any party, the originating organisation would be informed of the potential inaccuracy and asked to investigate and make the necessary changes to their data.

Information governance and security

Each partner organisation shall comply with Data Security & Protection Toolkit (DSPT) assertions, and make it a condition of employment that all staff (including assigned staff) who may have access to the health or social care record shall abide by the rules and policies of that organisation in relation to information governance.

This condition shall be written into relevant employment and other contracts and each partner organisation shall make staff aware that any failure to comply with the requirements outlined in this ISA is likely to be subject to disciplinary action. Partner organisations are responsible for ensuring that their staff who may have access to health or social care records are appropriately and regularly trained and are aware of this ISA and associated information governance arrangements.

Each partner organisation shall comply with:

- the DSPT as appropriate to its organisation type and adhere to robust information governance management and accountability arrangements, including effective security event reporting and management; and
- the requirement to annual self-assessment and regularly audit its compliance with the DSPT relevant to its organisation type, and report on its own assessment performance, relevant audits and improvement opportunities to the relevant Information Governance Group.

Each partner organisation shall audit Care Records access regularly in line with the requirements set by the DSPT.

Any partner organisation which is a non-NHS organisation and unable to comply with the DSPT shall obtain prior written approval from the *EoE IG Working Group* to adopt an alternative, but equivalent standard to the DSPT, for example, ISO 27001 / 2.

Access and Individual Rights

Those individuals whose personal data is being processed in accordance with this agreement have a legal right of access to their information. Where individuals make a subject access request for a copy of information held, or wish to raise any of their rights under data protection legislation this should be handled by the data controllers involved in the individual's direct care or in accordance with the joint controller agreement for any shared environment.

Responsibilities

Integrated Care Boards (ICBs) will;

- hold signed copies of this Agreement for each GP Practice and relevant partner organisations;

GP Practices will;

- promptly action requests from individuals wishing to object to their information being shared for direct care purpose.

All partner organisations will;

- ensure relevant Fair Processing Notices and other materials relating to *My Care Record can be easily accessed and* are clearly displayed at different points within relevant premises.

ICS IG Groups will:

- manage the leavers and joiners process advising their ICS organisations accordingly
- inform existing partner organisations of new organisations joining *My Care Record* and invite them to voice any objections or concerns, which must be addressed before the new organisation can join and be responsible for making sure that they meet the requirements of joining MCR, i.e., DSPT etc
- inform EoE IG Working Group of new organisations joining MCR
- regularly review the ISA in conjunction with EoE IG Working Group as per process flow maps

EoE IG Working Group will:

- sign off/approve any amendments to the ISA
- sign off/approve any new organisations or groups of organisations

Agreement start date

- 1st September 2022

Agreement review date

When there is a relevant change in circumstances, such as a change to legislation or geographical boundary changes. This Agreement is a rolling Agreement. This remains an active document until it is updated.

A general review would take place every 6 months.

Appendix A: Partner organisations

My Care Record involves local authority, NHS, social care or other health care providers.

Details of the organisations taking part can be found on the *My Care Record* website www.mycarerecord.org.uk.

Organisations will be added to the *My Care Record* website as they join the programme.

For the purposes of this document, these organisations can be included if they agree to principles and model highlighted in the ISA.

Appendix B: Definitions

The following definitions apply to this Agreement:

Term	Description	Source
Agreement	For the purposes of this document, this means '*My Care Record* Information Sharing Agreement'	Peer Review
Agreed Purpose	As defined in Table 1 of this agreement	Peer Review
Caldicott Guardian	A senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities providing social services must have a Caldicott Guardian	NHS Digital Data Security Standard 1
Common Law Duty of Confidentiality	When someone shares personal information in confidence, with a reasonable understanding that it will remain in confidence, it must not be disclosed without some form of legal authority or justification	UK Caldicott Guardian Council/Peer Review
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law	UK GDPR Article 4 (7)
Data Controller	See 'Controller'	UK GDPR Article 4 (7)
Data Flow Documents	Records that detail each use or sharing of personal information, including the legal basis for the processing	NHS Digital Data Security Standard 1
Data Processing	Any operation or set of operations which is performed on personal data or sets of personal, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction	UK GDPR Article 4 (2)

Data Protection Impact Assessment (DPIA)	A process carried out by the Controller using the advice of the DPO, when a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, prior to processing any data	UK GDPR Article 35 (1) (2)/Peer Review
Data Protection Legislation	All legislation and regulatory requirements in force from time to time relating to the use of Personal Data and the privacy of electronic communications, including, without limitation (i) any data protection legislation from time to time in force in the UK including the Data Protection Act 2018 or any successor legislation, as well as (ii) the General Data Protection Regulation ((EU) 2016/679) and any other directly applicable European Union regulation relating to data protection and privacy (for so long as and to the extent that the law of the European Union has legal effect in the UK)	Peer Review
Data Protection Officer (DPO)	A person with expert knowledge of Data Protection Law and practices who is appointed by the Controller/Processor to assist them in the monitoring of internal compliance with UK GDPR	UK GDPR Article 37-39 & Recital 97
Data Security & Protection Toolkit (DSPT)	An online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly	NHS Digital Data Security and Protection Toolkit (DSPT) website
Data Subject	Individual (natural person) who can be identified, directly or indirectly, by their personal data	UK GDPR Article 4 (1)
Direct Care	A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their	NHS National Data Opt-Out Operational Policy Guidance Document v4

	care	
EoE IG Working Group	Supports the delivery of MCR as the principle approach to the sharing of patient records and information for direct care purposes across the region	Peer Review
Fair Processing Notices	A defined set of information issued to data subjects by Controllers, where they hold and use their personal data, in a concise, transparent, intelligible, easily accessible form, using clear and plain language. Also known as 'Privacy Notices'	UK GDPR Articles (13) (14) ICO Guidance- Right to be Informed
GDPR	Legislation that is retained by domestic law and is now referred to as 'UK GDPR'.	Information Commissioner's Office
Information Commissioners Office (ICO)	UK's independent authority to uphold information rights and promote openness by public authorities and data privacy for individuals	ICO Website UK GDPR Article 51
Information Sharing Agreement (ISA)	Sets out the purpose of the data sharing, defines the data to be shared and sets out the standards and responsibilities of the parties involved, including the exercising of rights of the data subject.	UK GDPR Article 26 – Joint Controllers ICO – Data Sharing Code of Practice
Information Sharing Gateway - (ISG)	A website to improve and modernise the administration and risk assessment of information sharing in the public sector. Supports reporting on data flows and information sharing	Information Sharing Gateway Website
Integrated Care Boards (ICB)	The ICB is the Statutory Body that undertakes commissioning functions. It will also be accountable for NHS spend and performance within the system.	Health & Care Bill Policy Paper
ISO27001/2	An international information security management standard	ISO Website
Joint Controller Agreement	Agreement made between two or more controllers which defines their responsibilities	UK GDPR Article 26 (1)
Joint Controllers	Two of more controllers jointly determine the purposes and means of processing.	UK GDPR Article 26 (1)
Lawful Basis	Basis on which the controller processes personal data	UK GDPR Articles (6) & (9)
My Care Record	An approach to improving care and information sharing by joining up health and care information	*My Care Record* website/Peer

		Review
Partner Organisations	The organisations that are collaborating with each other within a specific shared environment as listed in Appendix A to this ISA and as updated from time to time	Peer Review
Personal Data/Information	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	UK GDPR Article 4 (1)
Role-Based Access & Control	A way of ensuring that system users are suitably authorised and access is appropriate to their roles	NHS Digital/Peer Review
Shared Environment	The different systems used by partner organisations to view the shared information	Peer Review
Source Systems	Each partner organisation's own health or social care database that holds personal or special category information	Peer Review
Special Category Data/Information	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation	UK GDPR Article 9 (1)
Subject Access Request	Request made to the controller to confirm whether their personal data is being process and if so, access to the personal data held	UK GDPR Article 15-Rights of access by the data subject

Appendix C: Data Protection Act/UKGDPR Principles/Definitions

Data Protection Act 2018/UKGDPR

Principle 1 - Fair and Lawful Processing

Each partner is individually responsible for ensuring its processing is fair and lawful.

Lawfulness - Each partner will ensure that patients are informed of how their patient identifiable information is used and shared.

For the sharing of patient identifiable information between the partners, the conditions for processing are:

- Lawful Basis - Article 6.1(e) UKGDPR:

  "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"

- Special Category Condition – Article 9.2(h) UKGDPR:

  "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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3"

Schedule 1 Part 1 Data Protection Act 2018 defines health or social care purposes as follows:

"Health or social care purposes

2 (1) This condition is met if the processing is necessary for health or social care purposes.

(2) In this paragraph "health or social care purposes" means the purposes of—

a. preventive or occupational medicine,
b. the assessment of the working capacity of an employee,
c. medical diagnosis,
d. the provision of health care or treatment,
e. the provision of social care, or
f. the management of health care systems or services or social care systems or services."

Each partner must ensure that its staff are subject to a duty of confidentiality equivalent to that which would arise if the person were a health professional.

Consent

In some circumstances, consent of the data subject may be obtained for establishing both a lawful basis and special category condition for processing patient identifiable information (Article 6(1)(a)).

Where consent is obtained this shall be specific to the service to be provided and shall be made clear to the data subject. The consent shall be recorded accordingly and shall be regularly reviewed (at least once on an annual basis).

Principle 2 - Purposes for processing

The Data is shared for the following health and care purposes and in order that each Partner may provide health and care services outside of the usual core contracted hours as set out in any General Medical Services (GMS) contract, Personal Medical Services (PMS) contract or, Alternative Provider Medical Services (APMS) contract, as held by that partner.

- To enable healthcare professionals to work efficiently and ensure that they have up to date information;
- To identify people with highly complex, multiple morbidity and/or frailty (and their carers), who might benefit from multi-disciplinary team support as part of case management and care planning;
- To identify and target specific service needs of patient groups, (e.g., for people with diabetes in order to improve their quality of care, experience of care and clinical outcomes);
- To identify suitable patients for the caseload of specialist nursing or medical services such as community geriatricians, matrons or mental health practitioners and, to reduce unnecessary unplanned admissions.
- To provide services to care homes in order to assist in the assessment and formulation of care plans and management.
- To guide each partner and their staff on how patient identifiable information can be shared lawfully;
- To explain the security and confidentiality laws and principles of information sharing and processing;
- To increase awareness and understanding of key issues;
- To support a process that will monitor, audit and review data access;
- To protect each partner from accusations of wrongful use of patient identifiable information.

Principle 3 - Adequacy and relevance

Patient identifiable information to be shared will be the complete record held on clinical system for shared patients. Information will be shared/accessed on a need-to-know basis when the requirements to view arises.

Principle 4 – Accuracy

Each partner agrees that:

- It is responsible for maintaining the personal information that it has collected on its own account, or jointly with another partner, in accordance with the Data Protection Act 2018 / UKGDPR;
- It will retain legal responsibility for correcting patient demographics and contact details where it is factually incorrect.
- It will not amend the record of an opinion or judgement recorded by a health or social care professional, whether accurate or not, because the recorded opinion or judgement is essential for understanding the clinical decisions that were made and to audit the quality of care;
- It will conduct a Data Protection Impact Assessment in accordance with UKGDPR and the Information Commissioner's Office (ICO) guidance on Data Protection Impact Assessments (DPIAs);
- It will complete The Data Security and Protection Toolkit to provide assurance that each partner is practicing good data security and that they are handling personal information correctly https://www.dsptoolkit.nhs.uk/

Principle 5 - Retention

Information will be held for the minimum amount of time in line with the records management code of practice. This will be in accordance with the Records Management NHS Code of Practice for Health and Social Care 2021 Records Management Code of Practice - NHSX

Where paper records are to be destroyed, this will be carried out in line with relevant national Information Governance protocols and guidance.

Principle 6 - Data Subject Requests

Where any partner receives a lawful subject access request (SAR) from a patient, this request will be forwarded promptly to the patient's registered practice who will be responsible for responding to the request. Where additional patient identifiable information is likely to be held by another partner to the ISA, patients will be provided with contact details for that other partner.

Each partner to this agreement should ensure that it has an effective procedure in place to respond to a SAR. Information about these procedures should be made available to all patients.

Each partner to this agreement must have a Data Protection Officer or an information governance lead who is responsible for subject access requests and complaints.

SARs from third partners for data available to organisations under this agreement are to be directed promptly to the Data Protection Officer or information governance lead of the relevant partner.

Principle 7 - Security

Each partner is responsible for applying appropriate technical and organisational security to its processing of patient identifiable information in order to meet its own obligations as data controller and requirements for processing NHS patient data. In particular, each partner shall as a minimum ensure that:

- Completion of the Data Security and Protection Toolkit is a requirement for all partners to the ISA. Completion of the Toolkit also meets the best practice guidance of the Information Commissioners Data Sharing Code of Practice.
- Staff only access patient identifiable information where they have a legitimate relationship with the patient and only authorised, appropriately trained staff may access patient identifiable information for the purposes of monitoring the quality or audit of the care delivered.
- The minimum necessary patient identifiable information is used to meet the particular data processing being carried out.

Any partner may inspect the security arrangements (as relevant to this ISA) of any other partner in order to satisfy itself of their adequacy, subject to reasonable notice and frequency. Where any partner fails (or expects to fail) to meet the standards of this ISA:

- All partners reserve the right to cease sharing patient identifiable information with that Partner unless and until the standards are demonstrably met.
- The partners may agree alternative assurances, considering the risks to a patient of not sharing and the risks to the information.

No partner may transfer patient identifiable information to countries which have not been assessed as 'adequate' under the UK GDPR.

Appendix D: Partners and Signatories for Information Sharing Agreement

Please accept your agreement to this via your Information Sharing Gateway Account or complete the below in CAPITAL letters.

I ..... (Name of Signatory {Caldicott Guardian or equivalent authorised signatory}) On behalf of:

Name of organisation: .....

Address line 1: .....

Address line 2: .....

Address line 3: .....

Postcode: .....

Organisation phone number:
.....

Organisation email address: .....

Organisation code: .....

Document Ref: v11

We hereby agree to the sharing of individual information/record for the provision/treatment of health and care.

To be signed by Caldicott Guardian or equivalent authorised signatory

Signature	
Name	
Job Role (e.g. Caldicott/SIRO)	
Date	
DPO Consulted (Please provide name)	

Any advisory amendments to the *My Care Record* would be emailed to you by the *My Care Record* team and updates would be provided on the website (www.mycarerecord.org.uk).

Updates would not require resigning of this Information Sharing Agreement, only legislative changes would require resigning of the Agreement.