My Care Record

Data Protection Impact Assessment (DPIA)

Table of Contents

MY CARE RECORD DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Introduction

My Care Record provides health and care professionals with electronic access to records of participating partner organisation, (see Appendix A of the MCR_ISA_0718/20) using new and existing secure computer systems for the purpose of direct care.

All partner organisations to the Information Sharing Agreement (ISA), will adopt the Data Protection Impact Assessment (DPIA) to ensure that they not only comply with the requirements of the General Data Protection Regulation (GDPR) but also to demonstrate that appropriate measures have been taken to ensure compliance.

The objective of the MCR DPIA is to identify and analyse the risks involved in the processing and sharing of information between partner organisations and how they ultimately affect the data privacy of individuals.

MY CARE RECORD DATA PROTECTION IMPACT ASSESSMENT (DPIA) FORM

Background Information			
Project/Activity Name:		**Date of DPIA submission:**	
Project/Activity Leads Name:		**Project/Activity Leads Contact Details:**	
Sponsor (e.g. Project Board):		**Lead Organisation:**	

Section 1: Identifying the need for a DPIA

Please complete this document in conjunction with the DPIA Guidance Document. The DPO should be consulted before completing a DPIA in order to provide specialist advice and guidance. The IG Manager/DPO must provide their comments (see 7.1 below) and must provide ongoing guidance should any review of a completed DPIA indicate outstanding or unmitigated risks or recommendations that require consideration prior to their acceptance or rejection.

What type of information are you sharing? ☒ Personal Identifiable ☐ Personal Non-Identifiable ☐ Business ☐Corporate
What is the Purpose?☒ Direct Care ☐ Indirect Care
Will the information sharing involve multiple organisations?☒ YES ☐ NO
Will the information sharing involve a large amount of personal data and affect a large number of data subjects?☒ YES ☐ NO
Will the information sharing involve the use of new or additional technologies? ☒ YES ☐ NO
Are the data to be shared revealing sensitive information as defined under the new GDPR legislation. Information such as, racial or ethnic origin, political opinions, religion or philosophical beliefs, or trade union membership, criminal convictions and offences or related security measures, genetic information, information concerning health or data concerning sex life? ☒ YES ☐ NO
Will personal information of vulnerable natural persons, in particular of children, be shared? ☒ YES ☐ NO

Will the information sharing involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data from multiple sources? ☒ YES ☐ NO
Does the information sharing involve using new technology which might be perceived as being intrusive? For example, the use of data to make a decision about care that's automated? ☐ YES ☒ NO

Section 2: Information Sharing/Data Flow Description

Give a brief description of the overall activity *My Care Record* provides health and care professionals with electronic access to records by participating partner organisations using new and existing secure computer systems. 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.
Are there Fair Processing/Privacy notices to enable information sharing? ☒ YES ☐ NO
Do you have a defined Subject Access Request (SAR) process in place? ☒ YES ☐ NO
List the types of personal data that will be shared 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
What is the purpose for sharing this data/information? 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.
How will the personal data/ information be transferred or shared between organisations? The data will be transferred on private N3, HSCN or via accredited secure networks in public sector networks.

Will you be transferring personal data to a country or territory outside of the EEA? ☐ YES ☒ NO
What is/ are the intended benefits/effects on individuals whose data will be shared? *MCR* provides individuals and health and care practitioners with the following benefits: • Better co-ordinated and seamless care therefore less repetition to health professionals • Quicker diagnosis and treatment • More time to spend on clinical care • Fewer unnecessary clinical tests • More accurate prescriptions • Safe and secure decision making
Will any data be hosted outside the UK ☐ **YES** ☒ **NO** **If yes, Please provide details to ensure appropriate compliance and data security.**
Identify partner organisations who will be subject to the agreements and who will have involvement/share responsibility for the data involved in this activity. Please see the *My Care Record* website www.mycarerecord.org.uk for details of the organisations who are taking part.
Is the data already held by the partner organisation? ☒ **YES** ☐ **NO** The partner agencies hold the records of their registered individuals. The records held by each partner connected electronically form an integrated care record.
How long will the personal data be held and how do you ensure that you are holding the data for the appropriate amount of time? Personal data will be held for the appropriate periods set out in NHS Digital's Records Management Code of Practice. The ISA requires the partner agencies to apply the IGA's Records Management Code of Practice retention periods and to follow its guidance on monitoring retention. This would vary according to the organisations and the types of data.

What technical security measures will be in place?

The measures required for compliance with the security requirements of the Data Security and Protection Toolkit. (The ISA requires all parties to have completed NHS Digital's Information Governance Statement of Compliance (IGSoC), which entails their compliance with the Toolkit.) and other relevant NHS standards and policies. Data would only be shared via N3, HSCN or via accredited secure networks in public sector.

Section 3: Consultation Process

Is your project driven by the statutory/legal obligations below?

☒ YES ☐ NO ☐ Not All (tick statutory Obligations you follow)

☐ General Data Protection Regulation (GDPR) (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 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 2016
☐ Health and Social Care Act 2012
☐ Health & Social Care (Quality and Safety) Act 2015
☐ Care Act 2014
☐ 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)

Purpose	Lawful Basis for Processing
Processing of Personal and Special Category information to be acquired from the provider systems and accessed across participating health and care organisations in support of direct care by participating partner organisations.	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 data is shared, the requirements of both GDPR and the law duty of confidentiality and other relevant legislation must be considered.	

Does the processing achieve the needed outcome?

☒ **YES** ☐ **NO**

Is there another way to achieve the same outcome?

☐ **YES** ☒ **NO**

Are there new purposes for processing information stated in the current ISA likely to be identified in the future? E.g. for the purpose of indirect care, not currently being used for direct care.

☒ **YES** ☐ **No**

Will any information stated in the ISA be transferred outside EEA?

☐ **YES** ☒ **NO**

What Systems /technologies will be used and How will data be held or stored?

The systems to be used include:
EMIS, VISION, TPP- SYSTMONE, MICRO TEST, CERNER HIE, PARIS, TIANI, LORENZO, ORION HEALTH, LIQUIDLOGIC, Mosaic supplied by Serverlec, SYSTEM C, SCR, SCRAI. The data is stored at the data centres of the partner agencies' systems suppliers. In some circumstances, it may also be held temporarily on the CERNER HIE.

Once new systems are introduced, the DPIA would be reviewed and updated.

What organisational measures are in place to ensure only appropriate and authorised access to, and use of, personal data?

Access will be controlled by username and password or role based access control (RBAC) where possible.
Health and care professionals with access will have contractual duties of confidentiality and be appropriately trained.

How will the system be audited for inappropriate access?

All partner organisations are required to follow the *My Care Record* Audit procedures for inappropriate access.

Section 4: Necessity, Compliance & Proportionality Measures

Is My Care Record GDPR compliant Fair Processing Notice available? **☒ YES ☐ NO**
Does this data sharing activity require permission from individuals where possible to view the records as best practice? **☒ YES ☐ NO**
Have individuals been given the opportunity to object to sharing? **☒YES ☐ NO**
What measures are in place in relation to internal reporting of a personal data breach? **All partner organisations would follow their internal policies and procedures for any data breach and take appropriate actions in line with their HR policies.**
Partner organisations would notify relevant signatories and the ICO within 72 hours where a breach/incident occurs relating to data shared. **☒YES ☐ NO**

Section 5: Identification & Assessment of Risks

Use the tables below to identify and detail a comprehensive list and level of risk associated with processing of data and the nature of potential impact on individuals.

Risk Scoring

		IMPACT				
		1) INSIGNIFICANT	2)MINOR	3)MODERATE	4) MAJOR	5) CATASTROPHIC
LIKELIHOOD		1	2	3	4	5
1) RARE	1	LOW	LOW	MEDIUM	HIGH	HIGH
2) UNLIKELY	2	LOW	LOW	MEDIUM	HIGH	EXTREME
3) MODERATE	3	LOW	MEDIUM	HIGH	EXTREME	EXTREME
4) LIKELY	4	MEDIUM	HIGH	HIGH	EXTREME	EXTREME
5) ALMOST CERTAIN	5	MEDIUM	HIGH	EXTREME	EXTREME	EXTREME

Risks associated with this Processing

Ref No.	**Privacy issue –** element of the initiative that gives rise to the risk	**(a) Risk to individuals** *(complete if appropriate to issue or put not applicable)*	**(b) Compliance risk** • *(complete if appropriate to issue or put not applicable)*	**(c) Associated organisation/corporate risk** *(complete if appropriate to issue or put not applicable)*
1	Individuals not adequately informed that their data is being processed and shared across the STP.	Some individuals may not be aware of or understand their choices.	Non-compliance with DPA principle 1 – fair and lawful processing	1. May lead to public mistrust 2. May lead to sanction by the Information Commissioners office (ICO)
2	The Health and Social Care Act 2012 provides a legal basis for the extraction of personal confidential data in certain circumstances. The sharing of personal confidential data from providers without consent carries the risk that individuals may lose trust in the confidential nature of the health service.	Some people may feel a loss of individual autonomy (no consent).	n/a	1. May lead to public mistrust
3	Data is disclosed to an unintended recipient	Some people may feel a loss of individual autonomy (no consent).		1. May lead to public mistrust

Risk Actions, Mitigation and Result of Assessment.

	Risk – taken from column (a), (b) and/or (c) in table 1.	Risk score – see tables at Appendix 2			Actions taken for solution(s)/mitigating action(s)	Result: is the risk accepted, eliminated, or reduced?
		Likelihood	Impact	RAG status		
1	Individuals not adequately informed that their data is being processed and shared across the STP. Non-compliance with DPA principle 1 – fair and lawful processing 1. May lead to public mistrust 2. May lead to sanction by the Information Commissioners office (ICO)	2	2	4	STP wide communications and engagement carried out with Fair Processing Notice, Website, Posters, Post Cards, Public Engagement events, Communications in newsletters and various Meetings. Communications materials were also distributed to GP practices to display in practices with merchandises (MCR branded Pens, Writing Pads, Hand Sanitisers, Coat Pins, Pull down banners and Mugs). In addition, internal partner organisations also created communications campaigns to inform on Intranet, posters, meetings etc. Communications has been ongoing for more than a year. All relevant staff informed of need to understand and disseminate communication material.	Reduced to an acceptable level (it is not possible to eliminate at this stage as communications is an on-going activity to enable individuals to be fully informed).

2	Some people may feel a loss of individual autonomy (no consent). Some individuals may not be aware of or understand their choices.	2	2	4	Awareness raising activities will help individuals understand their rights under GDPR and current data protection laws and how they can object to sharing. Website has FAQ section with details on ensuring individuals can make informed choice.	Accepted – There are processes in place to honour individuals rights to restrict the sharing of their personal information.
3	Data is disclosed to an unintended recipient	2	3	6	Security measures are implemented to ensure only clinical staff have access to system. Password protected access controls are in place with auditing for inappropriate access. Users are informed of consequences of inappropriate access during training.	Accepted – These are processes in place to honour individuals rights to restrict the sharing of their personal information. Health and care professionals are informed of consequences.

BLANK PAGE