Salford Clinical Commissioning Group

Salford Integrated Care Organisation

Data Protection Impact Assessment (DPIA)

Salford Integrated Record (SIR)

General Data Protection Regulation 2018

Data Protection Impact Assessment (DPIA)

Salford Integrated Record (SIR)

Version Control

Date Issue	20/12/17
Review Period	24 months
Review Date	20/12/19

Version History:			
Date	**Version Number**	**Author name and designation**	**Summary of main changes**
19/12/17	1	Based on SIR DPIA and edited where appropriate	First version
29/12/17	1_1	Updates from IG Associate	Minor amendments
4/10/2018	2_1	(Head of Information Assurance (SRFT)) (Head of Business Intelligence and Information Technology) NHS Salford CCG))	Review to align to GDPR requirements
Feb 2019	2_2	Additional final amendments reference to GMSS as host and SRFT as host of research database	Change to risk 5 (new host) addition of 4.11
June 2019	2~_3	Amendments made by Head of BI Caroline Rand suggested by GMSS	Minor amendments Typographical amendments updating IGT to DSPT and correcting legislation dates Additional clarity on research risk section

Contents

General Data Protection Regulation 2018
Data Protection Impact Assessment (DPIA):
Salford Integrated Record (SIR)

1. Overview

Data Protection Impact Assessment's (DPIA's) have been widely used in the UK, especially by government departments and agencies, local authorities, and National Health Service (NHS) organisations – these were previously knowns as Privacy Impact Assessments being good practice from the Information Commissioners Office (ICO), since the introduction of the General Data Protection Regulation 2018 have become mandated under the new legislation.

A Data Protection Impact Assessment (DPIA) is a process which enables organisations to anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions. Risks can be managed through the gathering and sharing of information with stakeholders. Systems can be designed to avoid unnecessary privacy intrusion, and features can be built in from the outset that reduces privacy intrusion.

A Data Protection Impact Assessment (DPIA) is intended to be a living document, with periodic review points general at times of change along the timeline of an initiative.

2. Requirement

This document includes the following annexes:

Annex one
Data Protection impact assessment screening questions

These questions are intended to help decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a full DPIA would be needed.

Annex two
Data Protection Impact Assessment template

This aims to assist the stakeholders when proposing change, to investigate whether the personal information aspects of their project/pilot/work program, etc. complies with the data protection principles in Chapter 2 of the General Data Protection Regulation 2018 (GDPR) (see Annex three).

Annex three
Linking the DPIA to Art. 5 GDPR Principles relating to processing of personal data

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the Data Protection legislation or other relevant legislation, for example the Human Rights Act.

General Data Protection Regulation Compliance – Sign Off
Signature page

The signature page should be completed and signed by the Partner leads the Information Governance support lead, and the other stakeholders.

3. Annex one

Data Protection Impact Assessment screening questions

These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be needed. It may become necessary to expand on answers as the project develops as part of the life cycle of the DPIA.

Will the project involve the collection of new information about individuals?

No – SIR will pull together existing data sets for partner organisations to give holistic view of patient records.

Will the project compel individuals to provide information about themselves?

Yes – will be shared digitally without data subject intervention

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Yes – other authorised partner organisations

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

No – all identifiable data used for direct care purposes

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

No

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

No - all identifiable data used for direct care purposes

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Yes – SIR will pool health and social care records

Will the project require you to contact individuals in ways that they may find intrusive?

No

4. Annex two

Data Protection Impact Assessment template

This template enables recording of the whole DPIA process. The template follows the process that is used in the Privacy Impact Assessment Code of Practice (from the ICO – Information Commissioners Office)

Step one: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

List who the stakeholders are (NHS and other public sector), including those who provide support to the work e.g. a software provider; a 'hosting' provider; etc.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions at Annex one).

Salford has an ambitious Integrated Care Programme for its residents, which consists of multiple projects that require IT solutions to underpin the organisational and procedural changes envisaged. A primary IT enabler that will need to be in place is a summary or shared care record which will enable all the partners to engage in safe, secure data sharing to better support residents and the professionals who provide their care.

The existing system will be upgraded. Graphnet CareCentric (CareCentric is the name of the product: Graphnet is the name of the supplier).

The NHS Salford Together:-Salford Integrated Care Advisory Board have recommended the record be called the Salford Integrated Record (SIR) and that it is seen as a direct care record which is not optional for patient care.

The following organisations are working together to bring social care, community, hospital and mental health service provision together, with a view to providing better, more integrated services and support for the full population within the City of Salford i.e. any Salford resident registered with a Salford CCG GP Practice (currently approximately 250,000 residents).

•Salford Royal NHS Foundation Trust (SRFT):
-Acute Services
-Secondary Care Services
-Community Services
-Adult Social Care (ASC) Services
•Salford City Council (SCC)
-Children's Social Care Services
• Greater Manchester Mental Health NHS Foundation Trust (GMMH)
-Mental Health Services
•Salford Clinical Commissioning Group (CCG)*
-45 GP Practice
•Salford Primary Care Together

* it is important to note that the CCG itself will not have access to Graphnet – CareCentric, or any Person Identifiable Data (PID) from it.

Although no new information about individuals will be collected, it will be processed in a new way and used by the Data Controllers in a much more safe and secure way than previously.

Although each partner organisation is Data Controller of their data, each must agree that as party to this shared SIR as a data controller in respect of personal data that it discloses, and as a data controller in common in respect of any information that it accesses in the SIR. GMSS & Graphnet & Salford Royal NHS Foundation Trust in their capacity as host, software provider and research host are data processors of personal data shared by any of the other partner organisations.

In support of the SIR, SRFT commissioned Mersey Internal Audit Agency (MIAA) to carry out an audit of the Information Governance arrangements, including data flow mapping and a review of information sharing agreements and processes, relating to the newly established Integrated Care Organisation (ICO). For reference, the report details are:

Integrated Care Organisation
Data Flow Mapping
Salford Royal NHS Foundation Trust
November 2016

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

The upgrade of the Salford Integrated Record (SIR) will be in phases:

Phase 1 SRFT and Salford CCG GP Practices

Phase 2 to add GMMH

Phase3 to add Social Care

An initial data upload is extracted and processed for inclusion in the SIR solution and this will be retained as a 'delta' feed. Changes to that data are replaced through near real-time or subsequent (time scheduled) data feeds. Data is linked on NHS number (and with other identifiers such as date of birth and postcode), then cleaned to form a new record, providing a longitudinal view of patient care.

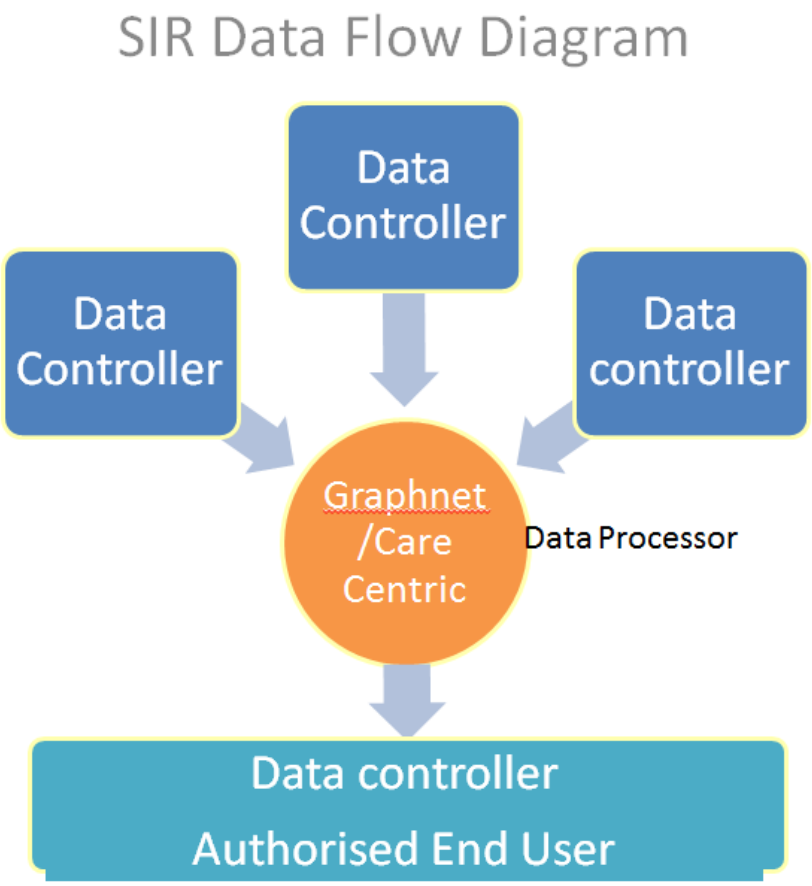
Users within each Data Controller local system will continue to access and update their current system, and in addition will see data in the SIR that is not from their own system (users will be able to see where the data is from). Both systems will be accessible from one user log in.

GMSS in its capacity as host will work with Graphnet to ensure that data is retained according to the Records Management Code of Practice, which is available on the Health & Social Care Information Centre website at: https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

Salford Royal in its capacity as host of research database ensure that a Data Processing Contract in line with GDPR requirements is in place with Graphnet an d relevant parties

The SIR will support the full population within the City of Salford i.e. any Salford resident registered with a Salford CCG GP Practice (currently approximately 250,000 residents).

A graphical representation of the data flows is set out below



NB GMSS is the main data processor using Graphnet software

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the DPIA process.

Various work is already underway for the purposes of establishing an Integrated Care Organisation (ICO), viz:-

Adult Social Care Services staff and data have already transferred to SRFT (on 1st July 2016).

There are currently two SIR Groups, both are chaired byChief Clinical Information Officer , who is the lead GP for Salford CCG:
-Salford Integrated Record Strategy Group - responsible for the future use of

data.
-Salford Integrated Record Governance Group - overall ownership of who has access, and what data extracts are allowed.

A SIR Information Governance Group can establish a task and finish group(s) as need arises. Membership to be made up from each partner organisation.

Salford CCG have also begun a range of SIR communications and engagement from Primary Care perspective, including:

- Members Bulletin
- Staff Bulletin
- Launch event
- Local face to face Presentations

There is continued Training and Awareness Raising as the SIR is rolled out and embedded into standard practice

A number of potential SIR privacy risks were identified during the MIAA audit dated 2016. A summary of these with recommendations are set out in the Report at Appendix G: Recommendations.

Step three: Identify the privacy and related risks

List which of the grounds in Article 6 are being relied on as providing a legitimate basis for processing personal data.

Please see the **Table 1 SIR DPIA Conditions**

Identify which of the grounds in Article 9 are being relied on as providing a legitimate basis for processing *sensitive personal data*?

Please see the **Table 1 SIR DPIA Conditions**

Please also see **Further support and a legal framework for the SIR** below, and **Appendix A - Data Sharing Law and Principles.**

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the Data Protection Legislation related compliance risks.

Please see the **Table 2 Identify the Privacy and Related Risks** below.

Table 1
SIR GDPR Conditions

There are two distinct stages to this **Sharing of Personal Records** work programme for the SIR:

1) ***bringing data together*** held in each electronic system by each partner organisation into the SIR
2) ***accessing data*** held by one or more of the partner organisations

The GDPR Conditions engaged for this are:

For bringing data together:	***For accessing data:***
ARTICLE 6 Conditions relevant for purposes of the first principle: processing of any personal data	
6(1.c) The processing is necessary for compliance with a legal obligation to which the data controller is subject 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 vested in the controller. .	6(1.c) The processing is necessary for compliance with a legal obligation to which the data controller is subject 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 vested in the controller.
ARTICLE 9 Conditions relevant for purposes of the first principle: processing of sensitive personal data	
9(2.g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; 9(2.h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services 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; (Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union	9(2.g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; 9(2.h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services 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; (Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to

or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies) * this includes registered Social Workers. 9(2.i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;	an obligation of secrecy under Union or Member State law or rules established by national competent bodies) * this includes registered Social Workers. 9(2.j) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

Further support and a legal framework for the SIR

Please see **Appendix A - Data Sharing Law and Principles** which sets out that as well as the General Data Protection Regulations, the Human Rights Act 1998, and the common law duty of confidence, the following support and provide a legal framework for bringing health and social care data together for the SIR:

- ✓ ICO Data Sharing Code of Practice: May 2011
- ✓ The Information Governance Review: March 2013
- ✓ Code of practice on confidential information: December 2014
- ✓ What does the Health and Social Care (Safety and Quality) Act 2015 do?
- ✓ Safe data, safe care: July 2016
- ✓ Review of data security in the NHS 2016
- ✓ Integrated Digital Care Records: Data Controller Issues 2016
- ✓ A Manual for Caldicott Guardians: January 2017
- ✓ Guidance on the NHS Standard Contract requirements on discharge summaries and clinic letters and on interoperability of clinic IT systems (2018)
- ✓ General Medical Council
- ✓ Nursing and Midwifery Council
- ✓ Health and Care Professions Council
- ✓ A narrative for Person – Centred Coordinated Care (NHS England)
- ✓ Next steps on the NHS Five Year Forward View March 2017
- ✓ Breaking down barriers to better heath and Care June 2018
- ✓ NHS long term plan – 2019

SIR Common Law Duty of Confidence Conditions

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges.

Three circumstances making disclosure of confidential information lawful are:
- where the individual to whom the information relates has consented
- where disclosure is necessary to safeguard the individual, or others, or is in the public interest
- where there is a legal duty to do so, for example a court order

As the SIR record is used to support direct care by a health or social care provider, there is no disclosure of the patient/clients personal information outside the team providing care.

Opt-out Model

The **Safe data, safe care** review of data security in the NHS, was published by the Care Quality Commission and the National Data Guardian in July 2016.

24 Recommendations were made, including an eight-point opt-out model, which sets out that:

- Information is essential for other beneficial purposes. Information about you is needed to maintain and improve the quality of care for you and for the whole community. It helps the NHS and social care organisations to provide the right care in the right places and it enables research to develop better care and treatment.
- You have the right to opt out of your personal confidential information being used for these other purposes beyond your direct care. This opt-out covers:

    A) Personal confidential information being used to provide local services and run the NHS and social care system.

    B) Personal confidential information being used to support research and improve treatment and care.

Please note that the opt-out will not apply to anonymised information. The Information Commissioner's Office has a Code of Practice that establishes how data may be sufficiently anonymised that it may be used in controlled circumstances without breaching anyone's privacy.

https://ico.org.uk/media/1061/anonymisation-code.pdf

Please see **Appendix A - Data Sharing Law and Principles** for further details.

http://www.cqc.org.uk/content/safe-data-safe-care

https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

National data opt-out programme

The national data opt-out is a new service that allows patients to opt out of their confidential patient information being used for research and planning.

The national data opt-out was introduced on 25 May 2018, enabling patients to opt-out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

By 2020 all health and care organisations are required to apply national data opt-outs where confidential patient information is used for research and planning purposes

While the SIR record supports direct care the application of “Opt out” codes is not applicable.

Table 2
Identify the Privacy and Related Risks

The risk scoring is based on the standard risk model below, where “C” is the consequence of the risk occurring based on different domains such Information Governance, and “L” is the likelihood. The risk score is calculated by multiplying C by L.

Consequence	Likelihood				
	1	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Consequence

	1	**2**	**3**	**4**	**5**
Description	**No Harm / insignificant**	**Very low harm / minor**	**Low harm**	**Moderate**	**Severe/Death**
Information Governance	Risk assessed as no harm/ insignificant. Less than 5 people affected.	Potential breach & risk assessed very low/minor. Up to 20 people affected.	Low breach of confidentiality. Up to 100 people affected.	Moderate breach with either particular sensitivity e.g. sexual health details, or up to 1000 people affected.	Serious breach with potential for ID theft or over 1000 people affected.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Likelihood

	1	2	3	4	5
Likelihood reflects how likely the consequence described will occur; either frequency or probability. % chance of recurrence of consequence in identified group.	This will probably never happen/recur Not expected to occur for years	Do not expect it to happen/recur but it is possible it may do so Expected to occur at least annually	Might happen or recur occasionally Expected to occur at least monthly	Will probably happen/recur, but it is not a persisting issue/ circumstances Expected to occur at least weekly	Will undoubtedly happen/recur, possibly frequently Expected to occur at least daily

1. Privacy risks to individual patients/clients.	Data breach.	L-3 C-4 Risk = 12 Moderate	ICO monetary penalty if breach of Principle 6. Reputational effect.
2. IG risks to individual clinicians/practitioners if there is poor quality or inaccurate data within the SIR.	Available information may be incomplete or insufficient. Lack of understanding how to use the information they see. Information overload - not seeing wood for trees.	L4 C4 Risk = 16 Moderate	ICO monetary penalty if breach of Principles 3 and 4.
3. Overall IG risks to Graphnet/Care Centric as system supplier.	Reputational damage if system does not deliver adequate protection of patient data.	L3 C5 Risk = 15 Moderate	ICO monetary penalty if breach of Principle 6. Reputational effect.
4. Key corporate IG risks to each partner organisation.	Public do not understand or believe in the need for the integrated record. Patients may raise concerns/complaints about the use of their data.	L2 C4 Risk = 8 Moderate	Reputational damage if system does not deliver. Lack of access to anonymised research data for partners as this is a key objective for the CCG. Partners do not find the product usable - wasted

			investment.
5. Additional IG risks to GMSS as the 'host' of the SIR.	Cyber security threats Physical and technical security threats.	L2 C5 Risk = 10 Moderate	All SIR complaints being targeted to the *host* organisation. Partners may not agree to or delay the sharing of data; disrupt project time scales or halt project. Bad press/reputational risk.
6. Failure to engage with the public /partners effectively.	Lack of trust, patients not comfortable with sharing their data on SIR. Patients not telling staff everything that they should, as they don't want it to be shared.	L4 C4 Risk = 16 Moderate	Patients and staff not understanding that it is legally permissible to create the SIR for health and social care. Bad press/reputational risk.
7. Failure of partners to have adequate information security standards in place.	Data is not securely protected, leading to data breaches. Loss of trust between individual and care organisations; failure to seek	L5 C4 Risk = 20 Severe	ICO monetary penalty if breach of Principle 6 Partners do not have assurance that processes are in place to enable safe data sharing; dependent on scale

	care in the future.		this could hamper delivery of the project.
8. Risks if we extract 'free text' data/information to be included in the SIR.	Content could contain sensitive data or third party data.	L4 C4 Risk = 16 Moderate	Content could include vital clinical information.
9. Sharing of third party information – this will be next of kin data, without their consent.	Breach of confidentiality.	L4 C3 Risk – 12 Moderate	ICO monetary penalty if breach of Principle 1 or 3. Breach Human Rights Act if excessive data is processed.
10. Risks if we only extract coded data to be included in the SIR.	Risk of inaccurate interpretation of coded data without contextual information.	L3 C3 Risk = 9 Low	Partners do not find the product usable - wasted investment.
11. Use of data for purpose other than direct patient care.	Loss of trust between individual and care organisations; failure to seek care in the future/ provide important details.	L2 C5 Risk = 10 Moderate	ICO monetary penalty if breach of Principle 1. Reputational effect. Breach of Human Rights Act and GDPR/DPA 2018
12. Failure to delete records for patients who have	Breach of Human Rights Act, GDPR, DPA 2018	L4 C4 Risk = 16 Moderate	ICO monetary penalty if breach of Principle 5.

moved out of area, have died or when a record has not been updated for 8 years.			Reputational effect.
Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
1. Privacy risks to individual patients/clients.	Correct access controls in place (RBAC). Monitor audit trail, and conduct audits on staff access. Information governance awareness and training to staff. Foster a culture for protecting SIR patient information within the ICO. Thorough investigation and complaints handling	Reduction L2 C3 Risk = 6 Low	Yes, it was: L-3 C-4 Risk = 12 Moderate

	procedures in place.		
2. IG risks to individual clinicians/practitioners if there is poor quality or inaccurate data within the SIR.	Mandatory training on use of coding standards - user groups. Evaluate the impact and effectiveness of training. Ensure a comprehensive information governance framework, policies, standard procedures and systems are in place and operating effectively within each ICO partner organisation. Use presentation and sorting function offered by CareCentric (software) - good training and onscreen notes for FAQ. Good practice - ask patient for clarification.	Reduction L3 C3 Risk = 9 Low	Yes, it was: L4 C4 Risk = 16 Moderate

3. Overall IG risks to Graphnet as system supplier.	Ensure testing of 'dummy' patient data before system goes live. Monitor data uploads for live patients.	Reduction L2 C5 Risk = 10 Moderate	Yes, it was: L3 C5 Risk = 15 Moderate So, Risk score has reduced.
4. Key corporate IG risks to each partner organisation.	Active IG programme management, including full DPIA and Information Sharing Agreement. Making sure that there is annual Information Governance /risk assessment in place and includes action plans. Clinical engagement of staff. Public engagement and transparency at all times. Post project user groups. Ensure right IG is in place for research and streamline access process to be slick and fully legal.	L1 C4 Risk = 4 Moderate	Yes, it was: L2 C4 Risk = 8 Moderate So, Risk score has reduced.

5. Additional IG risks to GMSS as the 'host' of the SIR.	Correct resources in place to manage this product. Conduct regular audits on Cyber security, physical and technical security threats. Test out Business Continuity Plans.	L1 C5 Risk = 5 Moderate	Yes, it was: L2 C5 Risk = 10 Moderate So, Risk score has reduced.
6. Failure to engage with the public /partners effectively.	Public engagement process. Consider ongoing public engagement via citizen panel etc. Robust communication plan in place; monitoring public involvement. Meetings to enhance partner's knowledge and engage support. Awareness raising of legal status for SIR. Engage all SIROs and Caldicott Guardians.	L3 C4 Risk = 12 Moderate	Yes, it was: L4 C4 Risk = 16 Moderate So, Risk score has reduced.

7. Failure of partners to have adequate information security standards in place.	Data Controllers to have organisational processes to maintain data security, and are compliant with the Data Protection Act 2018. If a partner organisation is not compliant with the data protection & security Toolkit, they should be excluded from the SIR (the SIR Board could grant access in exceptional circumstances, if they are satisfied that plans are in place to reach DSPT compliance). Withdrawal of SIR access if body fails to meet standards.	L3 C4 Risk = 12 Moderate	Yes, it was: L5 C4 Risk = 20 Severe
8. Risks if we extract 'free text' data/information to be included in the SIR.	Ensure better recoding, coding and analysis of data, so less or no free text information is needed. N.B. it is important that 'free text' data is extracted and made available in the SIR, as it may be essential to fully	L3 C2 Risk = 6 Low	Yes, it was: L4 C4 Risk = 16 Moderate

	understand the clinical needs of the patient. Without this information, there may be clinical risk issues.		
9. Sharing of third party information – this will be next of kin data, without their consent.	IG legal advice sought. Ensure fair processing. Limit to next of kin/ carer contact details.	L2 C3 Risk = 6 Low	Yes, it was: L4 C3 Risk – 12 Moderate
10. Risks if we only extract coded data to be included in the SIR.	Any data viewed must be checked with the patient and discussions held if it is to be used for critical clinical decision making.	L2 C3 Risk = 6 Low	Yes, it was: L3 C3 Risk = 9 Low So, Risk score has reduced.
11. Use of data for purpose other than direct patient care.	All *opt outs* must be honoured, for non-direct patient care. Data should be on 'need to know' basis. Warning alert should be set by IT to prevent unauthorised access to data. Block unauthorised access to data.	L1 C3 Risk = 3 Low	Yes, it was: L2 C5 Risk = 10 Moderate

	Clarity in communication about the purpose and use of the data - patient identifiable data for direct care only. ISA for direct patient care. DPIA for direct patient care. Need a formal streamlined process across all partners to manage requests. Pseudo-anonymised and anonymous data use permissible.		
12. Failure to delete records for patients who have moved out of area, have died or when a record has not been updated for 8 years.	Daily refresh from organisations will identify patients no longer on the GP Practice register/ no update in condition. Records of patients who have moved out of area, or when a record has not been updated for 8 years, should be deactivated and kept in a secured server, so staff are unable to view SIR record.	L2 C 2 Risk = 4 Low	Yes, it was: L4 C4 Risk = 16 Moderate

	Keep anonymised version for research purposes. Stipulation regarding compliance with GDPR principle 5.		

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Please see the **Table 3: Salford Integrated record delivered using Graphnet CareCentric- Risks log with actions.** below.

Table 3: Salford integrated record delivered using Graphnet CareCentric- Risks log with actions.

Risk number	Action reference	Action to be taken	Details of actions	Responsibility for action	Complete	Evidence
1	**Privacy risks to individual patients/clients.**					
1	1.1	Correct access controls in place (RBAC).	Administration rights clearly defined with roles	SIR Governance group controls group level access. EPR teams and GP		SLA with GMSS and local procedures

				teams control individual access based on this agreements.		
1	1.2	Monitor audit trail, and conduct audits on staff access.	EPR – in place	The SIR Governance Group will monitor access every 6 months.	Y	EPR procedure available. TOR SIR Governance and minutes
1	1.3		Other accesses – to be assessed.	Each partner using SSO to monitor access.		SIR board to approve procedures.
1	1.4	Information governance awareness and training	Toolkit evidence	Each partner/ CCG to monitor toolkit submissions		IG toolkit- BAU

		to staff.				
1	1.5	Foster a culture for protecting SIR patient information within the ICO.	Training programme	All partners. Training materials to users		Project to have a training workstream -
1	1.6	Thorough investigation and complaints handling procedures in place.	SRFT as Caldicott guardian to take on this role on Go live	SRFT		Further advice from MIAA Graphnet who accessed my data? Who does this?
2	**IG risks to individual clinicians/practitioners if there is poor quality or inaccurate data within the SIR.**					
Risk number	**Action reference**	**Action to be taken**	**Details of actions**	**Responsibility for action**	**Complete**	**Evidence**

2	2.1	Mandatory training on use of coding standards - user groups.	Each partner responsible for quality of their own data feed .Overall policy on data standards managed as part of locality & GM groups	SIR Strategy group top monitor data quality via DQ reports being commissioned by CCG from NWEH		SIR board
2	2.2	Evaluate the impact and effectiveness of training.	Project benefits	Project team		Project action

2	2.3	Ensure a comprehensive information governance framework, policies, standard procedures and systems are in place and operating effectively within each ICO partner organisation.	CCG to undertake annual audit and seek assurances including external audit of DSPT submissions.	CCG using NHS D DSP toolkit evidence		CCG/SIR board. / GMSS support on that .
2	2.4	Use presentation and sorting function offered by				Covered in training materials

		CareCentric (software) - good training and onscreen notes for FAQ.				
2	2.5	Good practice - ask patient for clarification.				Covered in training material
3	**Overall IG risks linked to Graphnet as system supplier.**					
Risk number	**Action reference**	**Action to be taken**	**Details of actions**	**Responsibility for action**	**Complete**	**Evidence**
3	3.1	Ensure testing of 'dummy' patient data before system goes live.	Started as part of project testing 15/10/18	SIR project board to monitor testing regime.		Project plan

3	3.2	Monitor data uploads for live patients.	GMSS as part of SLA for primary care. Trusts to monitor their own and report issues to GMSS	GMSS/ Trusts		GMSS GPs. Trusts monitor outgoing feed/ GMSS monitor incoming feeds
3	3.3	Ensure adequate data processing contract provision is in place with the software supplier (Graphnet)	GDPR compliant Data Processing Contract to be drawn up and signed by host partner and Graphnet	Host Partner		GMSS/ GM IDCR- assurance to the SIR board
4	**Key corporate IG risks to each partner organisation.**					

Risk number	Action reference	Action to be taken	Details of actions	Responsibility for action	Complete	Evidence
4	4.1	Active IG programme management, including full DPIA and Information Sharing Agreement.	SIR Governance board to schedule annual reviews			Project Annual SIR board
4	4.2	Making sure that there is annual Information Governance /risk assessment in place and includes action	CCG to lead	SIR Governance meeting		DPIA refreshed November 2018 and edited February 19.

		plans.				
4	4.3	Clinical engagement of staff.	Each partner responsible, user training materials	partners		Project seek assurance GMICDR – general principle SIR governance process for Salford.
4	4.4	Public engagement and transparency at all times.	All partners			GM programme. Salford Together/SRFT and CCG websites.
4	4.5	Post project user groups.				Local user group to be set up. Ask GM about wider user groups
4	4.6	Ensure right IG is in place for research and streamline access process	see action 1.6 and 2.3			SIR Governance board to restate process including any DPIA required .

		to be slick and fully legal.				
4	4.7	SRFT as host of research database must meet all security standards	SRFT demonstrate security	SRFT		SRFT to give written assurance annually with DSP toolkit and other security standards e.g. ISO2700
5	**Additional IG risks to GMSS as the 'host' of the SIR.**					
Risk number	**Action reference**	**Action to be taken**	**Details of actions**	**Responsibility for action**	**Complete**	**Evidence**
5	5.1	Correct resources in place to manage this product.	CCG/SRFT and GMSS part of SLA	GMSS/ Trusts		SLA in place
5	5.2	Conduct regular audits on Cyber security,	GMSS	GMSS		GMSS DSP Toolkit and working towards ISO2701

		physical and technical security threats.				
5	5.3	Test out Business Continuity Plans.	GMSS and local partners	GMSS and local partners		
6	**Failure to engage with the public /partners effectively.**					
6	6.1	Public engagement process. Consider ongoing public engagement via citizen panel etc.	CCG to lead			GM and SIR boards – GM has a public communications plan- Salford will be part of this. When this is clear we will follow with a Salford plan Results of “Big Conversations” on the website
6	6.2	Robust communication plan in place; monitoring public involvem	CCG to lead	SIR Governance		

		ent.				
6	6.3	Meetings to enhance partner's knowledge and engage support.				
6	6.4	Awareness raising of legal status for SIR.				
6	6.5	Engage all SIROs and Caldicott Guardians.				
7	**Failure of partners to have adequate information security standards in place.**					
7	7.1	Data Controllers to have organisational processe	partners	partners/ SIR Governance board see 2.3		DSPT evidence used by CCG as per 2.3

		s to maintain data security, and are compliant with GPDR				
7	7.2	If a partner organisation is not compliant with the Data Security and Protection Toolkit they should be excluded from the SIR (the SIR Board could grant access in exception	CCG to undertake annual audit and seek assurances including external audit of DSPT submissions.	SIR Governance group.		

		al circumstances, if they are satisfied that plans are in place to reach full IGT compliance).				
7	7.3	Withdrawal of SIR access if body fails to meet standards.		SIR Governance group.		
8	**Risks if we extract 'free text' data/information to be included in the SIR.**					
8	8.1	Ensure better recording, coding and analysis of data, so less or no free				GM ICDR and GM IG programme to manage

		text information is needed.				
9	**Sharing of third party information – this will be next of kin data, without their consent.**					
Risk number	**Action reference**	**Action to be taken**	**Details of actions**	**Responsibility for action**	**Complete**	**Evidence**
9	9.1	IG legal advice sought.				
9	**9.2**	Ensure fair processing.				
9	9.3	Limit to next of kin/ carer contact details.				GM issue - not extracted at present
10	**Risks if we only extract coded data to be included in the SIR**					
	10.1	Any data viewed must be checked with the patient and	users	part of training local professionals responsibility as		Local project training materials

		discussions held if it is to be used for critical clinical decision making.		part of their contract of employment		
11	**11. Use of data for purpose other than direct patient care.**					
Risk number	**Action reference**	**Action to be taken**	**Details of actions**	**Responsibility for action**	**Complete**	**Evidence**
	11.1	All *opt outs* must be honoured, for non-direct patient care.	SRFT BI team as guided by SIR Governance board and clear SLA			Need to update on national opt out processes SRFT ISG on working on his
	11.2	Data should be on 'need to know' basis.	Access is already governed by SIR Governance	SIR Governance board		

			board meeting all requirements			
	11.3	Warning alert should be set by IT to prevent unauthorised access to data. Block unauthorised access to data.				Refer to SRFT access process. ? audit by SIR group?
	11.4	Clarity in communication about the purpose and use of the data - patient				Update websites

		identifiable data for direct care only.				
	11.5	Need a formal streamlined process across all partners to manage requests.	SIR Governance board process has all partners engaged			
	11.6	Pseudo-anonymised and anonymous data use permissible.				SRFT can generate pseudonomised data but only they have the key making research extracts anonymised data using internal key.
12	**Failure to delete records for patients who have moved out of area, have died or when a record has reached legal retention period**					
Risk number	**Action reference**	**Action to be taken**	**Details of actions**	**Responsibility for action**	**Complete**	**Evidence**

12	**12.1**	Daily refresh from organisations will identify patients no longer on the GP Practice register/ no update in condition.	Tbc Graphnet as part of the service			GM board to provide assurance – to be managed at GM level with clarity required on who deletes these records
12	12.2	Records of patients who have moved out of area, or when a record has not been updated for 8 years, should be	Consult with Graphnet on system capability	GMSS		As above

		deactivated so staff are unable to view SIR record.				
12	12.3	Keep anonymised version for research purposes.	in line with risk 11	SRFT		
12	12.4	Stipulation regarding compliance with DPA principle 5. (record retention periods)	Update research guidelines	SRFT		Dir Board guidelines to be clear on retention periods

Step five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
Risks 1 to 12	As set out in *Step four: Identify privacy solutions* above.	Chief Clinical Information Officer SRFT.
Risks 1 to 12	As refreshed in section four; Identify privacy solutions above.	Chief Clinical Information Officer SRFT.

5. Annex three – Linking the DPIA to Art. 5 GDPR Principles relating to processing of personal data

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR other relevant legislation, for example the Human Rights Act.

First considerations:

Principle 1

a) Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject, shall not be processed unless:

a) at least one of the conditions in article 6 is met, and

b) in the case of special category data, at least one of the conditions in article 9 is also met.

The grounds for lawful processing relied upon as providing a legitimate basis for processing personal data are set out in Table 1"SIR DPIA Conditions" (page 11)

Have you identified the purpose of the project?

Yes, please see **Step one: Identify the need for a DPIA** above.

How will you tell individuals about the use of their personal data?

Please see **Consultation requirements** above

Do you need to amend your privacy notices?

No

Have you established which conditions for processing apply?

Yes, please see **Table 1 SIR GDPR Conditions** above.

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

The SIR does not rely on consent.

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

No

Have you identified the social need and aims of the project?

Yes, please see **Step one: Identify the need for a DPIA** above, and also **Step two: Describe the information flows** above.

Are your actions a proportionate response to the social need?

Yes

Principle 2

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

Does your project plan cover all of the purposes for processing personal data?

Yes

Have you identified potential new purposes as the scope of the project expands?

Yes

Will the project require you (or the host) to transfer data outside of the EEA?

No

Principle 3

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Is the quality of the information good enough for the purposes it is used?

Yes

Which personal data could you not use, without compromising the needs of the project?

The personal data already held by each organisation will be used, as described above in **Step two: Describe the information flows.**

Principle 4

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

If you are procuring new software does it allow you to amend data when necessary?

No, an initial data upload was extracted and processed for inclusion in the SIR solution and this will be retained as a 'delta' feed. Changes to that data are replaced through near real-time or subsequent (time scheduled) data feeds, from each partner organisation.

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Each Data Controller is responsible to keep the data held in their system as accurate.

Principle 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');.

What retention periods are suitable for the personal data you will be processing? These should be taken from the 'Records Management: NHS Code of Practice' which is available from the Department of Health at: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

The Code of Practice will be used.

Are you procuring software that will allow you to delete information in line with your retention periods?

Yes

Principle 6

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Do any new systems provide protection against the security risks you have identified?

Yes

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Staff with access to the SIR will receive training to enable them to operate the SIR.
Partner Organisation with access to, or sharing data through the SIR will maintained general Information Governance training for all staff

Second Consideration:

The SIR board shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Compliance

Is there documented evidence of compliance with the data protection principles?

The SIR board provides assurance that the conditions set out in the DPIA are implemented, reviewed and adhered to

Proof

Where processing is based on consent there is need to demonstrate that the data subjects have consented to processing of his or her personal data (Article 7(1))

The SIR does not rely on consent.

Obligation

Article 6 (4) Lawfulness of processing

4. Where the processing **for a purpose other than that for which the personal data have been collected** is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, **take into account**, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

The SIR data shall not be further processed in identifiable form

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

The SIR data shall be collected from the clinical systems of the partner organisations under secure and tested data flows.

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9

The SIR data sets will contain person identifiable information as described in Article 9. Processing of these data sets is outlined in table 1

(d) the possible consequences of the intended further processing for data subjects;

The SIR data shall not be further processed for any purposes outside that of direct care of the data subjects.

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

The SIR data shall be held on secure N3 servers, with current security standards applied.

Appendix A - Data Sharing Law and Principles

Background and Overview

As well as the Data Protection Act 1998, the Human Rights Act 1998, and the common law duty of confidence, the following support and provide a legal framework for bringing health and social care data together in a shared record.

Everything contained in this Appendix has been taken in summary from the full version of each section of this Appendix. Live web links are also included, to reference the full versions if required.

In summary, this Appendix provides a short history for sharing health and social care data:

- ✓ Best practice
- ✓ Professional guidance
- ✓ Codes of Practice
- ✓ Principles
- ✓ and Law

ICO Data Sharing Code of Practice: May 2011

https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

The public sector

Produced by the Information Commissioner Office (ICO), this Code sets out that most public sector organisations derive their powers entirely from statute – either from the Act of Parliament which set them up, or from other legislation regulating their activities.

The Information Governance Review: March 2013

https://www.gov.uk/government/publications/the-information-governance-review

Information: To share or not to share?

This Government Review provided a revised list of Caldicott Principles, with the new 7th Principle:

> *The duty to share information can be as important as the duty to protect patient confidentiality.*

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

There are four legal bases that may provide an organisation with a justification for holding and using personal confidential data. All processing of such data must be lawful. There are four legal bases for processing personal confidential data which meet the common law duty of confidentiality. These are:

1. with the consent of the individual concerned. Details concerning consent for direct care are fully explored in chapter 3;
2. through statute, such as the powers to collect confidential data in section 251 of the NHS Act 2006 (see section 6.7) and the powers given to the Information Centre in the Health and Social Care Act 2012 (see sections 1.8, 6.5 and 7.3.4).
3. through a court order, where a judge has ordered that specific and relevant information should be disclosed and to whom; and
4. when the processing can be shown to meet the 'public interest test', meaning the benefit to the public of processing the information outweighs the public good of maintaining trust in the confidentiality of services and the rights to privacy for the individual concerned.

In addition to having one of these legal bases the processing must also meet the requirements of the Data Protection Act and pass the additional tests in the Human Rights Act.

The revised list of Caldicott Principles

https://www.gov.uk/government/publications/the-information-governance-review

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

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

These principles should underpin information governance across the health and social care services.

Code of practice on confidential information: December 2014

http://digital.nhs.uk/cop

Published by the Health and Social Care Information Centre

This code of practice describes good practice for organisations handling confidential information concerning, or connected with, the provision of health services or adult social care. It therefore has a particular scope.

This code of practice is provided in response to the Health and Social Care Act 2012, section 263.

The Code includes guidance on:

- Individuals' objections to the handling of information about them
- Information held under an obligation of confidence
- Dispose of information once it is no longer required

The Health and Social Care (Safety and Quality) Act 2015: Duty to share information

http://www.legislation.gov.uk/ukpga/2015/28/section/3/enacted

In Part 9 of the Health and Social Care Act 2012 (health and adult social care services: information), after section 251A (as inserted by section 2 of this Act) insert—

251B Duty to share information

(1)This section applies in relation to information about an individual that is held by a relevant health or adult social care commissioner or provider ("the relevant person").

(2)The relevant person must ensure that the information is disclosed to—

(a)persons working for the relevant person, and

(b)any other relevant health or adult social care commissioner or provider with whom the relevant person communicates about the individual,

but this is subject to subsections (3) to (6).

(3)Subsection (2) applies only so far as the relevant person considers that the disclosure is—

(a)likely to facilitate the provision to the individual of health services or adult social care in England, and

(b)in the individual's best interests.

(4)The relevant person need not comply with subsection (2) if the relevant person reasonably considers that one or more of the following apply—

(a)the individual objects, or would be likely to object, to the disclosure of the information;

(b)the information concerns, or is connected with, the provision of health services or adult social care by an anonymous access provider;

(c)for any other reason the relevant person is not reasonably able, or should not be required, to comply with subsection (2).

(5)This section does not permit the relevant person to do anything which, but for this section, would be inconsistent with—

(a)any provision made by or under the Data Protection Act 1998, or

(b)a common law duty of care or confidence.

(6)This section does not require the relevant person to do anything which the relevant person is required to do under a common law duty of care (and, accordingly, any such requirement is to be treated as arising under that common law duty and not under this section)."

What does the Health and Social Care (Safety and Quality) Act 2015 do?

https://digital.nhs.uk/information-governance-alliance/resources/information-sharing-resources

Published by the Information Governance Alliance

The new Act reinforces existing good practice and obligations on health and social care professionals and provides statutory support for the seventh Caldicott principle that – "the duty to share information can be as important as the duty to protect patient".

It makes it clear that unless an individual objects, when information can be lawfully shared between health or adult social care commissioners or providers for purposes likely to facilitate the provision of health services or adult social care and are in an individual's best interests, then it must be shared.

Safe data, safe care: July 2016

http://www.cqc.org.uk/content/safe-data-safe-care

Report into how data is safely and securely managed in the NHS

This thematic review, published by the Care Quality Commission (CQC) and the National Data Guardian (NDG), of data security was conducted to establish whether personal health and care information is being used safely and is appropriately protected in the NHS.

Data security, in this review, is defined as:

- Availability
- Integrity
- Confidentiality

Review of data security in the NHS 2016

http://ukcgc.uk/docs/caldicott3.pdf

Published by the Care Quality Commission and the National Data Guardian

Recommendations

24 Recommendations were made, including:

> *There should be a new consent / opt-out model to allow people to opt out of their personal confidential data being used for purposes beyond their direct care. This would apply unless there is a mandatory legal requirement or an overriding public interest.*

(see the eight-point opt-out model below).

The National Data Guardian's Data Security Standards

These 10 National Data Guardian's Data Security Standards are intended to apply to every organisation handling health and social care information, although the way that they apply will vary according to the type and size of organisation.

Leaders of all health and social care organisations should commit to the following data security standards. They should demonstrate this through audit or objective assurance, and ensure that audit enables inspection by the relevant regulator.

Leadership Obligation 1

People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standards 1 to 3.

Leadership Obligation 2

Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standards 4 to 7.

Leadership Obligation 3

Technology: Ensure technology is secure and up-to-date.

Data Security Standards 8 to 10.

The eight-point opt-out model

https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

1. You are protected by the law. Your personal confidential information will only ever be used where allowed by law. It will never be used for marketing or insurance purposes, without your consent.

2. Information is essential for high quality care. Doctors, nurses and others providing your care need to have some information about you to ensure that your care is safe and effective.

However, you can ask your health care professional not to pass on particular information to others involved in providing your care.

3. Information is essential for other beneficial purposes. Information about you is needed to maintain and improve the quality of care for you and for the whole community.

It helps the NHS and social care organisations to provide the right care in the right places and it enables research to develop better care and treatment.

4. You have the right to opt out. You have the right to opt out of your personal confidential information being used for these other purposes beyond your direct care.

This opt-out covers:

A) Personal confidential information being used to provide local services and run the NHS and social care system.

B) Personal confidential information being used to support research and improve treatment and care.

This choice could be presented as two separate opt-outs. Or there could be a single opt-out covering personal confidential information being used both in running the health and social care system and to support research and improve treatment and care.

5. This opt-out will be respected by all organisations that use health and social care information. You only have to state your preference once, and it will be applied across the health and social care system. You can change your mind, and this new preference will be honoured.

6. Explicit consent will continue to be possible. Even if you opt out, you can continue to give your explicit consent to share your personal confidential information if you wish, for example for a specific research study.

7. The opt-out will not apply to anonymised information. The Information Commissioner's Office has a Code of Practice that establishes how data may be sufficiently anonymised that it may be used in controlled circumstances without breaching anyone's privacy.

The ICO independently monitors the Code. The Health and Social Care Information Centre, as the statutory safe haven for the health and social care system, will anonymise personal confidential information and share it with those that are authorised to use it.

By using anonymised data, NHS managers and researchers will have less need to use people's personal confidential information and less justification for doing so.

8. Arrangements will continue to cover exceptional circumstances. The opt-out will not apply where there is a mandatory legal requirement or an overriding public interest.

These will be areas where there is a legal duty to share information (for example a fraud investigation) or an overriding public interest (for example to tackle the ebola virus).

Integrated Digital Care Records: Data Controller Issues 2016

https://digital.nhs.uk/information-governance-alliance/resources/information-sharing-resources

Published by the Information Governance Alliance

Who are the Data Controllers for NHS Patient Data?

Data controller in common arrangements have been introduced in a number of areas, often to build shared buy in to the delivery of a project by reassuring participants that they remain in control of the data they share.

Two different models are considered here. The first involves information being transferred to a central hub where the collated record is then made available to participating organisations. The second involves system functionality enabling participating organisations to view a snapshot of records created in another organisation.

In either model it is necessary to consider, for each participating organisation including system suppliers:

- Is the organisation participating under a written contract that prevents it from processing data other than under the instruction of a separate data controller? If so it is a data processor.
- If not a data processor, to what extent does the organisation determine the purposes that data are used for? To which data does this apply? At what point do they start and/or stop determining the purposes that any particular data are used for? Do they have any say over what each other does?
- Separately, consideration needs to be given to the extent that each organisation determines the way in which the data are processed. To what extent is this determined by a system supplier? To what extent does the organisation determine the way in which a partner organisation processes data?

Information Sharing Agreements should cover:

- The assurances required by the organisations that use the system in respect of its security as individually they are unlikely to be able to specify and manage system security;
- Clarification of the legal obligations falling on each organisation using the system, including accuracy of the information they contribute;
- Clarification of expected working practices within each organisation (linked to IG Toolkit requirements)
- Reciprocal agreements in respect of additional – non-legally binding - services for patients

A **Checklist of Key Issues** is provided as Appendix 1 to this guidance to support health and care communities adopting a data controller in common model. The checklist can be found at:

https://digital.nhs.uk/information-governance-alliance/resources/information-sharing-resources

Appendix 2 to this guidance provides a list of responsibilities, derived from the Data Protection Legislation but also the common law and other areas of law and sets out, at a high level, the system requirements that organisations need to develop or procure when implementing integrated digital care records.

A Manual for Caldicott Guardians: January 2017

https://www.gov.uk/government/groups/uk-caldicott-guardian-council

Produced by the UK Caldicott Guardian Council

Legal and ethical aspects

The legal aspects which Caldicott Guardians particularly need to be familiar with are the Data Protection Act and the common law duty of confidence. Other relevant legislation is described in Annex C.

Legal considerations

Personal information may be shared legally in one of three ways:

● with the consent of the individual concerned (providing that individual has mental capacity: see Annex C);

● when it is required by law (e.g. The Children's Act 1989 requires information to be shared in safeguarding cases);

● when it is in the public interest.

The use of patient information in research

Those participating in research will normally give informed consent for participation in the research, but should also be informed about and give consent for the uses to which the information collected about them during the research will be put.

Person-identifiable information used for research must comply with the provisions of the Data Protection Act.

Whenever possible, person-identifiable information should not be used for research or audit purposes.

Where to find help and guidance

Annex B of the Manual for Caldicott Guardians 2017 sets out where to find help and guidance.

General Medical Council

http://www.gmc-uk.org/

The General Medical Council (GMC) has published (Wednesday 25 January 2017) revised, expanded and reorganised guidance on confidentiality for all doctors practising in the UK. The guidance – Confidentiality: good practice in handling patient information – comes into effect from Tuesday 25 April 2017.

Revisions have been made to the guidance, last published in 2009, following an extensive consultation exercise. While the principles of the current GMC guidance remain unchanged, it now clarifies:

- The public protection responsibilities of doctors, including when to make disclosures in the public interest.
- The importance of sharing information for direct care, recognising the multi-disciplinary and multi-agency context doctors work in.
- The circumstances in which doctors can rely on implied consent to share patient information for direct care.
- The significant role that those close to a patient can play in providing support and care, and the importance of acknowledging that role.

The GMC has also published a decision-making flowchart and explanatory notes to show how the new guidance applies to situations doctors may encounter and find hard to deal with, such as reporting gunshot and knife wounds or disclosing information about serious communicable diseases.

Confidentiality: good practice in handling patient information is available on the GMC's website.

https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality

Nursing and Midwifery Council

https://www.nmc.org.uk/

'The Code for nurses and midwives' provides guidance on safeguarding, confidentiality, and sharing information with other healthcare professionals.

https://www.nmc.org.uk/standards/code/

> 5 Respect people's right to privacy and confidentiality
>
> *As a nurse or midwife, you owe a duty of confidentiality to all those who are receiving care. This includes making sure that they are informed about their care and that information about them is shared appropriately.*

Health and Care Professions Council

http://www.hpc-uk.org/

Regulating health, psychological and social work professionals. 'Our standards of conduct, performance and ethics' are the ethical framework within which HCPC registrants must work. It is important that registrants read and understand this document".

http://hpc-uk.org/publications/standards/index.asp?id=38

> *2.6 You must share relevant information, where appropriate, with colleagues involved in the care, treatment or other services provided to a service user.*

Guidance on the NHS Standard Contract requirement on discharge summaries and clinic letter and on interoperability of clinical IT systems

https://www.england.nhs.uk/wp-content/uploads/2018/09/interoperability-standard-contract-guidance.pdf

2.2 this is defined in the Contract as structured clinical information relating to significant aspects of a Service User's health, care or treatment, held by the

Provider within Service User Health Records and identified in Guidance published by NHS Digital and/or NHS England from time to time as information to be made available, as appropriate, through open interfaces to other providers of health and social care

A- Narrative for Person Centred Coordinated Care

https://www.england.nhs.uk/wp-content/uploads/2013/05/nv-narrative-cc.pdf

Person centred coordinated care "I can plan my care with people who work together to understand me and my carer(s), allow me control, and bring together services to achieve the outcomes important to me."

NHS long term Plan

https://www.longtermplan.nhs.uk/

Next Steps on the NHS Five Year forward view

https://www.england.nhs.uk/wp-content/uploads/2017/03/NEXT-STEPS-ON-THE-NHS-FIVE-YEAR-FORWARD-VIEW.pdf

Technology to support the NHS priorities

To ensure that patients get the right care in the most appropriate location, it is also important that clinicians can access a patient's clinical record. By December 2017 every A&E, Urgent Treatment Centre and ePrescribing pharmacy will have access to extended patient data either through the Summary Care record or local care record sharing services.

Breaking down barriers to better health and care

https://www.england.nhs.uk/wp-content/uploads/2018/06/breaking-down-barriers.pdf

Working in partnership

To make this happen, all parts of local systems – such as GPs, care homes and home care, hospitals, community and mental health services – are working together more closely than ever before. They have come together to form local 'sustainability and transformation partnerships' in every part of England, to run services in a more coordinated way, to agree system-wide priorities, and to plan collectively how to improve residents' day-to-day health.

6. **GDPR Compliance – Sign Off**

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the GDPR.

The partner organisations are all legally registered Data Controllers in their own right.

These Data Controllers will come together to provide health and social care for their patients/clients/service users. There are no Information Governance concerns in this respect, as they all have a legitimate relationship with the patients/clients, in providing their care and treatment.

For bringing data together, and for accessing data, the Conditions set out in **Table 1 SIR GDPR Conditions** above are satisfactorily met.

If this Data Protection Impact Assessment concerns patient data, the **Caldicott Guardian*** should also be one of the signatories.

If this Data Protection Impact Assessment concerns staff data, the **Senior Information Risk Owner*** (SIRO) should also be one of the signatories.

If this Data Protection Impact Assessment concerns data being hosted by a **non-NHS organisation**, the SIRO* should also be one of the signatories.