Joined Up Care Derbyshire

# Data Protection Impact Assessment (DPIA)

| | |
|---|---|
| Name: | [redacted] |
| Job Title: | IG Leads Derbyshire SCR Project |
| Title of project being assessed: | Derbyshire Shared Care Record Proof of Concept |
| Division/Corporate Team: | Joined Up Care Derbyshire |

Data Protection legislation makes it mandatory to perform a Data Protection Impact Assessment (DPIA) in case of large scale processing of special category data (for example health data). The identification of a legal basis is also needed before you start processing data; therefore a DPIA is required and should document the legal basis to be relied upon.

Under Data Protection legislation both Data Controllers and Processors have responsibilities and can be liable for any breach of the regulation, even though it remains that the Controller determines the purpose.

**Brief description of the aim / desired outcome / purpose of the project**:

The purpose of this document is to ensure that the Derbyshire Shared Care Record (DSCR) system is implemented with consideration of all data protection/privacy laws. The document helps to identify, understand and manage or mitigate any privacy risks while allowing the aims of the project to be met. **This assessment relates to the initial Proof of Concept (PoC) which is to be delivered by Orion Health. This DPIA will need to be reviewed, updated and re-approved in relation to Phase 2 of the Derbyshire Summary Care Record Project.**

The aim of the Derbyshire Shared Care Record is to integrate health and social care so that people, patients and carers only have to tell their story once. Sharing information electronically, it will offer direct access for authorised health and social care professionals to provide as full a picture as possible of an individual's history, needs, and support and service contacts.

Information will only be shared when it is needed to make direct care and treatment easier and faster. This will help to provide seamless integrated care and fulfil our obligations under the Care Act 2016.Information will be 'view only' in one complete record for the person containing all health and social care data from all source systems. The GP record will be accessible unless the person previously chosen not to share this data from their own GP surgery.

**For the PoC phase, the only information that will be shared is the current Medical Interoperability Gateway (MIG) dataset that is already shared between partner organisations. No additional information will be shared as part of the PoC and so the current Derbyshire MIG Information Sharing Agreement can be used. This ISA will need to be updated and re-approved prior to phase 2 of the DSCR. There will also be no population health management (secondary use) functionality delivered as part of the PoC.**

The DSCR is a key digital enabler for the Sustainability and Transformation Partnership (STP) known as Joined Up Care Derbyshire (JUCD https://joinedupcarederbyshire.co.uk/about/what-is-jucd ) – a national initiative that drives sustainable transformation in health and wellbeing for Derbyshire residents.

This document has been developed in consultation with the Derbyshire Information Governance Workstream. It is an evolving document which will be regularly refreshed and developed as the programme of work continues. Significant amendments to the document will be outlined and approved by the IG Workstream. Overall sign off of the document and identified risks will be by each organisation Data Protection Officer/Caldicott Guardian/SIRO, managed by their internal processes.

There are future phases of the DSCR and linked projects which will require future iterations of this document or related DPIAs to be development. These include secondary use of data, including business intelligence and patient portal.

**Does the project involve any 3rd party suppliers or partners?**
If Yes, who are they and what is their role?

- Orion Health are the approved supplier for delivery of the Derbyshire Shared Care Record.
- Healthcare Gateway are the providers of the MIG which is currently in use across Derbyshire and which will be used to provide the proof of concept.

**What personal data will be processed?**

| | Personal Data | Yes | No | Notes |
|---|---|---|---|---|
| 1. | Hospital or NHS number | ☒ | ☐ | |
| 2. | Name | ☒ | ☐ | |
| 3. | Date of birth | ☒ | ☐ | |
| 4. | Contact details (e.g. address, telephone numbers, email address) | ☒ | ☐ | |
| 5. | Gender | ☒ | ☐ | |
| | **Special categories of personal data** | **Yes** | **No** | **Notes** |
| 6. | Data concerning health | ☒ | ☐ | |
| 7. | Data concerning sex life or sexual orientation | ☒ | ☐ | |
| 8. | Genetic or biometric data | ☐ | ☐ | |
| 9. | Racial or ethnic origin | ☒ | ☐ | |
| 10. | Religious or philosophical beliefs | ☒ | ☐ | |
| 11. | Approximately how many people will we collect data about? | Less than 100 | ☐ | Between 100-500 ☐ |
| | | Between 500-1,000 | ☐ | Between 1,000-10,000 ☐ |
| | | Between 10,000-50,000 | ☐ | More than 50,000 ☒ |

**Describe the scope and nature of the processing:**

1. What is the source of the data?
2. How will you collect, use, store and delete data?
3. Will you be sharing data with anyone? If yes who?
4. You might find it useful to refer to a flow diagram or another way of describing data flows.

The key organisations which make up the 'partners' of the DSCR are:

- NHS Derby and Derbyshire Clinical Commissioning Group (CCG)
- GP Practices across Derbyshire
- Chesterfield Royal Hospitals NHS Foundation Trust
- University Hospitals of Derby and Burton NHS Foundation Trust
- Derbyshire Community Health Services NHS Foundation Trust
- Derbyshire Healthcare NHS Foundation Trust
- Derbyshire Health United
- Derby City Council
- Derbyshire County Council

For the proof of concept, patient information (see below) will be viewable via the MIG, through the Orion portal. This information is already available to organisations through the MIG, with no additional information being included for the PoC.

| |
|---|
| Patient demographics |
| Summary, including current problems, current medication, allergies, and recent tests |
| Problem view |
| Diagnosis view |
| Medication including current, past and issues |
| Risks and warnings |
| Procedures |
| Investigations |
| Examination (blood pressure only) |
| Events consisting of encounters, admissions and referrals |

This data (Above) is based on the minimum requirements of what is necessary for patients receiving care in an urgent, out-of-hours setting. This data does not include free text.

End of life care/ supportive care datasets, outlined in the supporting document, does include freetext which has no character limit.


HGQM023 MIG Supportive Care Data

Access to the portal will be available either via a single sign-on from the organisations clinical system (and therefore directly related to the patient currently accessed on the system) or through a user login to the Orion portal.

No Third Party will have access to the data at any point as a result of the DSCR, unless named as a partner organisation and as outlined in the Information Sharing Agreement or a relevant Data Processing Agreement/overarching contract.

**Rights of data subjects:**

1. What is the nature of your relationship with the individuals?
2. How much control will they have?
3. Would they expect you to use their data in this way? i.e. is it in line with Trust Patient or Staff privacy notices
4. Do they include children or other vulnerable groups?

The data within the DSCR PoC will relate to patients/service users within each partner organisation, including children and vulnerable groups. Each organisation will have access to data only when they have a legitimate relationship with the data subject. A user would only be able to see a patient/service user record relating to their organisation, unless they have a legitimate/lawful basis or patient consent for accessing the record.

GDPR, DPA18, Common Law Duty of Confidentiality and other Health Service legislation determine how organisations can use personal information. The Health and Social (Safety& Quality) Act 2015 set out the duty for information to be shared with other professionals where it facilitates the care for an individual and it is legal to do so.

In general, subjects expect their care information to be shared and professionals will only share information if directly relevant to the provision of care and in the best interests of the subject. Clinicians and care providers have a legal duty and professional obligation to respect privacy and keep information confidential in the course of care delivery. Service users have the right to confidentiality and privacy and expect professionals to keep their data safe and secure.

Patients/service users can dissent from their data being share into the DSCR, however individuals need to be made aware of the benefits of the system and the risks involved with not sharing the data with other professionals involved in their care.

A robust Fair Processing activity, through various channels of communication, has already taken place across Derbyshire with the roll-out of the MIG. For the PoC, there is no requirement for additional patient communications as no additional information is being shared and no additional organisations/partners are included in the scope of the processing.

**Lawful basis for processing**

**Health and Social Care Act 2012**

All health and adult social care providers are subject to the statutory duty under section 251B of the Health and Social Care Act 2012 to share information about a patient for their direct care. This duty is subject to the common law duty of confidence, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

**Common Law Duty of Confidence**

For common law purposes, **sharing information for the DCR is on the basis of implied consent**.

The DCR will allow sharing for direct care to become more reliable and systematic, but it will not change the legal basis of implied consent. Implied consent to access relevant information about the patient, or to share it with those who provide (or support the provision of) direct care to the patient can be relied on as a legal basis if the following conditions are met:

- The information being shared or accessed is to provide or support the individual patient's direct care.
- Information is readily available to patients, explaining how their information will be used and that they have the right to object.
- There is no reason to believe the patient has objected.
- The information is shared in confidence.

**GDPR**

Under GDPR there must be a valid lawful basis to process personal data. For GDPR sharing information for the DCR is **on the basis of public task** where "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 6(1)(e) of the GDPR is the condition for lawfully processing data for delivering direct care as part of the DCR:**
**6(1) (e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…**'

Article 9(2)(h) of the GDPR is the condition for processing 'data concerning health' (personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status) for direct care as part of the DCR:

**9(2) (h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'**

The DCR will use an additional 'permission to view' model whereby a person can consent to access their record at the point of care with a legitimate professional treating them.

**Safeguarding**
There are legal provisions that support the release of data for the purposes of safeguarding children and vulnerable adults. The Children Acts 1989 and 2004 establishes implied powers for local authorities to share information to safeguard children, safeguard and promote the welfare of children within their area who are in need, and to request help from specified authorities including NHS organisations. The Care Act 2014 sets out a legal framework for how local authorities and other parts of the health and social care system should protect adults at risk of abuse or neglect.

For GDPR, in addition to the Articles 6(1)(e) and Article 9(2)(h) cited above, there is an additional provision for sharing data for the purposes of safeguarding, as follows:

**9(2)(b) …'is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of…social protection law in so far as it is authorised by Union or Member State Law …'**

**Describe compliance and proportionality measures, in particular:**

1. Does the processing actually achieve your purpose?
2. Is there another way to achieve the same outcome?
3. How will you ensure data quality and data minimisation?
4. How will you prevent function creep?
5. What information will you give individuals?
6. How will you help to support their rights?
7. What measures do you take to ensure processors comply?
8. How do you safeguard any international transfers?

The purpose of the DSCR is to enable secure sharing of identifiable service user health and social care data between the partners of the project. Currently, the information that will be shared would be made available to these professionals through local record sharing, the MIG or on request. The DSCR speeds and simplifies the process, allowing identified professionals access to essential or urgent information without a lengthier request procedure.

All health and care professionals accessing information in the DCR will have/required to have a legitimate relationship with the person whose information they are accessing, i.e. they are directly responsible for providing health or social care for that person.

**For the proof of concept, the information sharing will use the Medical Interoperability Gateway (MIG) which therefore means that only coded information (apart from some textual information related to end of life care) will be shared.**

**Governance**

Each Data Controller will have appropriate technical and organisational measures in place to comply with Article 5 (f). The Information Sharing Agreement will outline agreed standards ensuring each partner will take reasonable steps towards appropriate technical and organisational security measures. This requirement will also be somewhat illustrated by each partner organisation being complaint with NHS Digital Data Security and Protection Toolkit (DSP Toolkit).

A legally binding contract will be in place with the supplier and will include standard contract clauses and assurances regarding security in order for this principle to be complied with. IG leads of the partner organisations will be involved and provided the opportunity to review the relevant section of the contract through their membership of the Derbyshire IG Workstream Group.

**Availability**
Information within the DSCR will be a duplicate; in the event of a failure recovery procedure will revert back and extract a copy of the source data. In case of non-availability of the system, previous methods of information sharing will entail (for example email, telephone). The Orion portal is hosted by Amazon Web Services in the UK. Multiple data centres are used by AWS in the UK to ensure availability of information and services should one data centre fail.

**Accuracy**
Each Data Controller will be responsible for the accuracy, completeness and quality of the information held in their systems, which in turn feed in to the DSCR. Each Data Controller must have processes in place to ensure that there are regular opportunities for records to be updated and for accuracy and completeness to be maintained.

**Up to Date**
Accuracy of the data in the DSCR will have a dependency on the regularity of the extract. Regular extracts will result in improved accuracy and reliability of DSCR content as changes in the source systems will be captured. Data within the DSCR system will be refreshed either near real time or at least every 24 hours – depending on the provider.

**Identification of Risks**

This table identifies the privacy and related risks involved with the DSCR. The table below outlines the mitigating factors for each risk and whether they adequately reduce/eliminate the risks highlighted, along with the required actions to be implemented.

| Identified risk | Risk to individuals | Compliance risk | Solution/Mitigation |
|---|---|---|---|
| Citizens not fairly and suitably informed of how their data will be processed. | Damage and/or distress<br>Uninformed | Article 5 (1) (a) - Principle 1 lawful, fair and transparent | MIG sharing/fair processing information already available. Further/updated fair processing campaign to be suitably presented.<br><br>Fair processing communications and formats suitable for all age groups and demographics.<br><br>Comprehensive training for relevant staff to ensure queries and concerns can be dealt with. |
| Processing occurs with no suitable legal basis. | Damage and/or distress | Article 5 (1) (a) - Principle 1 lawful, fair and transparent<br><br>Article 6 (1)<br>Article 9 (1) | Legal basis identified and agreed between the data controllers before processing begins. |
| The data is processed outside of the agreed purpose (Direct Care). | Damage and/or distress<br>Privacy intrusion | Article 5 (1) (b) – Principle 2 specified, explicit, legitimate | The purpose will be clearly defined within the DPIA and ISA and supplier contract.<br>Future phase to cover the sharing for secondary use within the DSCR will require update to DPIA/ISA. |

| | | | |
|---|---|---|---|
| DSCR system users have access to data where there is no basis or justification to do so. | Damage and/or distress | Article 5 (1) (c) – Principle 3 adequate, relevant, limited to what is necessary.<br><br>Article 5 (1) (f) - Principle 6 security of personal data | Role based access and view will be determined by clinical need. DSCR will require a robust audit facility.<br>Each partner organisation will be responsible for monitoring and auditing access of their users. The ability to run audit reports must be allocated to an individual within each organisation and appropriately trained. |
| Confidentiality of a citizens full health and social care record at risk if DSCR security jeopardised. | Damage and/or distress | Article 5 (1) (f) - Principle 6 security of personal data | The technical specification for the system includes all applicable security requirements to prescribed industry standards, including penetration testing, business continuity and disaster recovery plans. These are outlined in the contract and when requested supplier should provide guarantees that such measures are in place. The written contract with the supplier outlines strict security standards.<br><br>Security measures are outlined within the ISA and the contract held with the system supplier.<br><br>All users of the DSCR must be up to date with annual IG training.<br><br>Password parameters for access to the DSCR will be decided and agreed upon through the Derbyshire IG Workstream Group. |

**Sign Off and Outcomes**

| Item | Name / Date | Notes |
|---|---|---|
| **Risk approval:** | | If accepting any residual high risk, consult the ICO before going ahead. |
| **Data Protection Officer (DPO) advice given by:** | | DPO should advise on compliance, risks assessed and whether processing can proceed. |
| **Summary of DPO advice:** | | |
| | | |
| **Comments:** | | |
| | | |