Dorset Care Record
Partner Data Sharing Agreement

CONTENTS

1 INTRODUCTION

The Dorset Care Record (DCR) is a local health and social care record which brings together information from participating Health and Care organisations. The DCR is a key component of the data sharing requirements of the Dorset Integrated Care System (ICS). The Pan Dorset Information Governance Group oversees the data sharing arrangements across the ICS and data sharing via the DCR is part of the ICS sharing framework.

The DCR record is a copy of health and care information held by the participating organisations.

The DCR holds data for people who are registered patients of a General Practice in the Dorset ICS and also for people who have received treatment from any organisation that contributes data to the DCR. Registered patients of a General Practice in the ICS are referred to below as 'DCR data subjects'.

The DCR enables timely access to key information in the health and social care records of DCR data subjects. This ensures that health and social care staff can access health and care history, including, but not limited to, data, correspondence, medications, allergies, test results and social care information in order to make well informed decisions that are in the best interests of DCR data subjects.

The DCR will be linked to the Hampshire and Isle of Wight shared care record (ShCR), the Care and Health Information Exchange (CHIE). When the interoperability links are in place, a user of the DCR will also see data available within the CHIE for the patient they have selected. Users of the CHIE will also see any data held in the DCR for the patients they are accessing, both will be presented alongside each other in the users consolidated viewer. This will provide a direct care benefit for patients living in one county and receiving care in another county.

Changes to the DCR as a result of regional data sharing will be managed through the DCR governance process, as set out in section 14 below and will be in line with the principles set out in this agreement.

This Data Sharing Agreement (DSA) covers use of data for clinical and care purposes only. Any proposed further uses of the data not related to direct care will be discussed with, and only take place with the written explicit approval of the joint data controllers.

2 PARTIES TO THE AGREEMENT

The invited parties to this agreement, otherwise known as 'the Partners' are listed in appendix 1.

3 PURPOSE

This Agreement sets out the framework for the sharing of personal data between the Partners. It defines the principles and procedures that the Partners shall adhere to, and the responsibilities that the Partners owe to each other.

The Partners agree to only process shared personal data for the sole purpose of the provision of direct care. The aim of the data sharing initiative will serve to promote

positive health and wellbeing outcomes for data subjects by making care and treatment easier, faster, and more effective.

The parties will not process shared personal data in a way that is incompatible with the purpose described in this clause.

4 CONTROLLERSHIP OF DATA

The control of data shared via the DCR is a joint arrangement with the organisations that constitute the Partners identified as joint data controllers for the DCR data.

Not all organisations contributing data to the DCR are partners. These organisations are 'contributing' controllers and not part of the joint controller arrangements, (noting that the joint controllers are also likely to be contributors). Their influence over decisions regarding data on the DCR extend as far as agreeing that the data they contribute can be shared for the purposes stated in this agreement. They are in control of determining what data they contribute from their systems.

The link between the DCR and the CHIE when sharing data regionally does not form a joint controllership arrangement between the two care records. Each county is responsible for their own data controllership in accordance with the NHS Guidance at the time of updating this DSA - Information Governance Framework: Shared Care Records - NHS Transformation Directorate (england.nhs.uk)).

The following table sets out the responsibilities of the joint controllers of the DCR data and notes how these responsibilities are addressed:

Area of responsibility	**Joint Controller requirements**	**Current status**
Individuals are informed about the use of the shared record	Develop common materials for partners to link to	Provided by the DCR website and citizen engagement strategy
Data is processed lawfully	Define the shared purposes for use of the data via this agreement.	Set out in Data Sharing Agreement
Data used for limited purposes	Establish agreed purposes and if necessary, a process to identify, assess and agree other uses with the controllers.	Set out in Data Sharing Agreement
The minimum data is used	Ensure design of the system provides the minimum necessary data to end users	Set out in Data Sharing Agreement and agreed dataflows with each contributor
Data is accurate	Ensure processes to link and display data do not compromise accuracy	Existing processes to load and check data in the DCR
Data retained only as long as necessary	Ensure shared record does not retain data for longer than appropriate periods	Set out in Data Sharing Agreement and the DCR

Area of responsibility	Joint Controller requirements	Current status
		Records Management and Retention Policy
System security control definition	Identify risk and design appropriate control measures to secure the shared record	Set out in Data Protection Impact Assessment and related security specific documents
System security management	Application of any requirements when setting up users and ensuring the security of data processor activities	Set out in Data Protection Impact Assessment and related security specific documents
Encryption & pseudonymisation	Determination of applicability as risk controls and implementation where possible	Set out in Data Protection Impact Assessment and related security specific documents and applied by Orion
Resilience & restoration	Determination of applicability as risk controls and implementation where possible	Set out in Data Protection Impact Assessment and related security specific documents and applied by Orion
Security audits are undertaken	Security controls as defined in the DPIA are audited to assure effectiveness	By Orion (penetration tests etc) and DCR Team
Usage audits are undertaken	Provision of audit reports to support organisational audit activities	By the DCR team
All access is by authorised users only	Process to ensure all access is authorised	Set out in DSA & DPIA and user management procedures across all partners
Maintaining records of processing (ROPA)	Hold records of all data contributions and access controls	DSA, DPIA and other policies all relate. Also detailed data extracts and processing by Orion is documented
Breach notification	Notify any breaches to all affected partners and agree co-ordinated response	Operational procedures of DCR team.
Impact Assessment	Conduct DPIA on the data processing. Maintain any changes or additional processing. Audit risk control measures – share with all partners	DPIA is in place and periodically reviewed
Support Data Subject Rights	Agree and maintain joint processes to support any requests related to ICR data	Data Subject rights covered in DSA and team processes

The responsibilities of any contributing controller are to:

- confirm the sharing purposes are lawful uses of the data they control;
- ensure the sharing is covered in their Fair Processing Activities;
- agree the framework of purposes that the data they share can be used for;
- ensure the data they share is the minimum necessary;
- ensure reasonable endeavours for data extracts to be accurate and timely;
- ensure data shared has not exceeded the retention period;
- highlight any risks they identify to the DCR programme;
- ensure appropriate set up of authorised end users;
- ensure own compliance with the Data Security & Protection Toolkit is maintained;
- audit own user activities;
- hold records detailing the data they contribute;
- notify any breaches to joint controllers for co-ordination.

All organisations whose staff access the DCR, whether they contribute data or not, are responsible for ensuring their staff make appropriate use of the DCR in line with the purposes, legal bases and requirements of this sharing agreement and that user access is appropriately set up and managed.

4.1 Data Processors

The following organisation(s) shall act as data processors, under the instruction of the joint data controllers.

Organisation	Orion Health Ltd
Role	Software Vendor
Address	1 King St, Hammersmith, London, W6 9HR

5 DEFINITIONS

For the purposes of this specific agreement, the definitions used are as set out in Article 4 of UK GDPR [1] these include:

[1] https://gdpr-info.eu/art-4-gdpr/

‘Personal Data’ means any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’;

‘Data Controller’ means the natural or legal person, public authority, agency or other body which, alone ‘or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law’;

‘Data Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller’.

‘DCR Data Subject’ means a registered patient of a general practice in the Dorset Integrated Care System.

6 THE DATA TO BE SHARED

The following types of personal data will be shared between the parties during the term of this agreement:

- basic personal identifiers (e.g. name, date of birth and contact details of the data subject);
- identification data (i.e. NHS number of individual receiving treatment);
- any other information that may be necessary to share for the purposes of providing direct care.

The following types of special categories of personal data will be shared between the parties during the term of this agreement:

- data in a person's health and care record.

Any changes to the data shared shall be considered and agreed through the governance process set out in this document.

Signatories to this document are in agreement that the data shared from their organisation via the DCR will also be available in the CHIE, where the patient has a record in both systems.

7 GENERAL OBLIGATIONS ON ALL PARTIES

In accordance with the principles of the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018, the contributing data controller undertakes to ensure only the minimum necessary amount of personal identifiable data (PID) is shared in the DCR for the purposes it is used for.

Controllers whose staff access the DCR undertake to ensure data is only accessed by those with a legitimate reason. The joint data controllers confirm that facilities exist in the software used to process the PID to make such restrictions of use according to the clinical or care role of the user.

All parties need to ensure the use of PID does not cause a breach of confidence under the common law duty of confidentiality. Where use of data is related to the direct care of the individual and they are generally aware, then confidentiality is not breached. This is achieved by activities to inform individuals and also where the access by the user is within the reasonable expectations of the public.

Meeting the requirements of UK GPDR, the DPA 2018 and common law duty of confidentiality is also likely to meet the requirements of the Human Rights Act 1998 of the right to respect for their private and family life.

Should DCR data subjects feel that processing of their data infringes upon their rights and freedoms, they may exercise the right to object or request that the processing of their data is restricted.

The Health & Social Care (Safety & Quality Act) 2015 provides an express duty to share information, where information can be lawfully shared in line with data protection law and common law duty of confidence, and the information facilitates the provision of health services and adult social care, unless the data subject objects.

All parties are responsible for ensuring that their own organisational and security measures protect the lawful use of information shared under this Agreement.

All parties agree to inform the DCR team of any actual or suspected breach of confidentiality or incident involving a risk or breach of the security of information in the DCR as soon as possible and within 24 hours of discovery. The DCR team will then notify all affected parties so that the appropriate investigation and action can take place. The investigation will seek to establish the nature of the breach including numbers affected and the items of data involved. Following initial investigation and where relevant, the data controller(s) likely to be at fault will be required to consider informing the ICO and the affected data subjects within the timeframes stipulated under UK GDPR.

All parties agree to provide reasonable assistance to other parties in investigating incidents and undertaking appropriate remedial action.

8 LAWFUL, FAIR AND TRANSPARENT PROCESSING

8.1 Lawful Bases

The lawful bases for processing data in the DCR under UK GDPR Article 6 are set out below:

6(1)(e) – '*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'*[2]

6(1)(c) – *processing is necessary for compliance with a legal obligation*[3]

[2] For example, S.72 of National Health Service Act 2006 *'It is the duty of NHS bodies to co-operate with each other in exercising their functions.'*
Health and Social Care (Safety and Quality) Act 2015 *'Duty to share information' (where not otherwise constrained by law).*

[3] For example, S.11 of Children Act 2004 – health and social care organisations *'…must make arrangements for ensuring that their functions are discharged having regard to the need to safeguard and promote the welfare of children; and any services provided by another person pursuant to*

In some emergency medical situations the following basis would also apply:

6(1)(d) – '*processing is necessary to protect the vital interests of a data subject or another person'*

8.2 Special Category Personal Data

The lawful basis for processing special category personal data under UK GDPR Article 9 will be:

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*[4] *or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in [UK GDPR Article 9] paragraph 3*'[5]

Or in some circumstances:

Article 9(2)(i) '*processing is necessary for reasons of public interest in the area of public health'*

In some emergency medical situations the following legal basis would also apply:

9(2)(c) '*processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent'*.

The above bases for processing are linked to the Data Protection Act 2018 Schedule 1, Part 1, paragraph 2 (d-f) related to the provision of health or social care and management of health or social care systems and services.

8.3 Fair and Transparent Processing

The parties acknowledge that in line with the stipulations of;

- the UK General Data Protection Regulation (UK GDPR);
- Principles One & Eight of the Caldicott Principles,

personal data must be processed fairly and lawfully. This means that data subjects should not be surprised by what information is being shared, why that information is being shared and with whom it is being shared.

The DCR website includes information about the DCR, including a Privacy Notice in order to meet their fair processing obligations, and instructions on how to exercise data subjects' rights.

---

arrangements made by the person or body in the discharge of their functions are provided having regard to that need.'

[4] See footnote 2 above.

[5] this refers to use of data by bodies/persons that are subject to confidentiality through their professional registration or employment contract.

The joint data controller assists data controllers in meeting their fair processing obligations by maintaining an open access website at Dorset Care Record which describes the use and content of the DCR and provides a mechanism by which members of the public can raise an objection to the sharing of their data;

Data Controllers undertake to promote these materials or to make equivalent information available to the public to comply with the requirement for fair processing.

9 USERS AND USER ORGANISATIONS

In order to access the DCR, the user must be providing a direct health or care service for or on behalf of a person who is a DCR data subject, as defined in Section 1. Organisations outside of the Dorset community will provide some services to DCR data subjects via regional or national data sharing initiatives.

9.1 User Organisations

An organisation may be given access to the DCR, directly or via regional or national data sharing requirements, if they:

- provide a health or care service to DCR data subjects. This will include organisations outside of the Dorset ICS area provided their access is for the provision of a health or care service to a DCR data subject. This access may be via direct access to the DCR, or via the DCR being linked to other care record systems, e.g. via the CHIE;
- have attained 'Standards Met' in the Data Security and Protection Toolkit (DSPT), or equivalent if they are an organisation not required to complete a DSPT;
- have signed and agreed to abide by the terms of a Data Sharing Agreement with the DCR;
- undertake only to request access for staff who meet the criteria set out in section 9.2 below;
- are registered with the Information Commissioner's Office;
- are CQC accredited, if appropriate;
- train staff on their induction as to their responsibilities under UK GDPR and other data protection legislation, and undertake refresher training at least annually;
- ensure that all staff have confidentiality clauses in their Contract of Employment.

Organisations may qualify regardless of whether they are NHS, local authority, voluntary sector or commercial health or care organisations (including Care Homes, Hospices and high street Pharmacies), providing they meet the criteria above.

In accessing or sharing data with the DCR, the data controller acknowledges that they meet the criteria set out above. The data controller also acknowledges that other parties meeting these criteria may be given access to data held in the DCR, including the data supplied by themselves.

9.2 Users

In order to qualify as a user of the DCR an individual must:

- be trained in the use of the DCR;
- receive annual training in information governance and data security and protection;
- not further share the data with any other parties;
- process the shared personal data in accordance with technical and organisational security measures, together with any other applicable laws and guidance;
- have confidentiality clauses in their Contract of Employment;
- understand that they are authorised only to access data for DCR data subjects with whom they have a legitimate care relationship;
- understand that data subjects have a right to request access to the audit trail which will detail users who have accessed their record in the DCR or via the CHIE;
- understand that their continued employment and, where relevant, professional qualification may be at risk if they access information inappropriately, and that this may also be illegal and subject to criminal proceedings.

10 AUDIT

Where appropriate the data processor undertakes auditing and testing of the DCR, and provides the ability to audit access to information held on the DCR. This may be done both;

- proactively, to investigate possible errors in records or to check for inappropriate access; and
- reactively, where questions have been raised about appropriate use of the system or the quality of data.

All data subjects whose records are available in the DCR have the right to request the audit trail which details who has accessed their record in the DCR or via the CHIE through the interoperability programme.

The contributing data controller(s) agree that audit trail information may be supplied to other contributing data controllers and to data subjects regarding the activities of employees of the contributing data controller's organisation. If there are any concerns about the disclosure of the audit trail to the data subject, the organisations to which the audit trail pertains should be consulted.

11 OBJECTION TO THE USE OF DATA FOR DIRECT CARE

Data Subjects may object to sharing their data through the DCR for their care. As a result, there is a balance required between respecting the objection of individuals and accepting a risk of their health or care data not being readily available. At present the

joint data controllers respect the wishes of individuals expressed through an objection and will act on these by preventing information from being accessible in the DCR or outside of county borders.

The decision to automatically respond to data subjects' objections by opting them out of the service will be kept under review in the light of developing best practice and data sharing and citizen engagement strategies.

Under this agreement the data controller agrees to inform data subjects who wish to object about their options to do so by directing them to the fair processing materials available to ensure that this is a fully informed decision. The data controller agrees to make data subjects who object aware that doing so may have a detrimental impact on the ability of a health or social care professional to treat them in the best possible way.

11.1 Withdrawal of Objection

The parties acknowledge that objections to data processing via the DCR can be reversed at the request of the data subject, or their representative and agree to operate the procedures to do so where required.

12 DATA QUALITY AND RETENTION

Should any parties identify any inaccurate data held in the DCR, they will immediately notify the DCR team in order that timely rectification of the data can be facilitated.

Data will be retained by the DCR in accordance with the DCR Retention Policy which complies with the NHS Records Management Code of Practice 2021.

13 DATA SUBJECT RIGHTS

13.1 Right of access:

If any requests are received for access to information that has been fed into the DCR from partner organisations, the relevant partner organisations will be informed and required to respond directly to the requestor. As the DCR is not a primary source system itself, it is not currently considered appropriate that it be the source for subject access requests (SARs). This position is based the application of the serious harm test (DPA 2018) whereby any access request for health records falls to the healthcare professional responsible for the care and treatment to which the data relates. The serious harm test cannot be determined by a central team.

13.2 Rectification:

If any part of an individual's record is believed to be incorrect, either by the individual themselves or an end user, then that concern must be addressed by the original source organisation. Any concerns raised to the DCR programme will be passed to the relevant source organisation to check and if required, amend the data. Where technically possible amendments will feed through to the DCR. Where that is not possible, the DCR programme will assess and as required seek to correct the data within the DCR.

13.3 Erasure

The right to erasure of health and care records is limited. Should any contributing partner to the DCR erase part of the records provided, where technically possible this will carry through to the DCR. Where that is not possible, the DCR Programme will assess and as required mark the record beyond use.

There is no automated correction/removal of data functionality available within the ShCR system, in compliance with ICO guidance.

13.4 Restriction & Objection

These rights are covered in Section 11 above.

13.5 Portability & Automated Decision Making

These rights do not apply to the data held in the DCR.

14 GOVERNANCE PROCEDURES

The DCR Programme Board will oversee this agreement, supported by the Pan Dorset IG Group for subject matter expertise.

15 CHANGES TO THIS AGREEMENT

15.1 Termination

This Agreement will terminate in the event of and upon early termination of the DCR Partner Agreement.

The DCR Programme Board may decide to terminate this Agreement in accordance with its governance and decision-making arrangements.

A Partner, which is considering terminating its participation in this Agreement, shall notify the DCR Programme Board of its intention and reasons, and agrees to liaise with the DCR Programme Board for at least one month, before giving notice of termination, to ascertain whether its concerns can be addressed. Having done so, a partner may terminate its participation in this Agreement by giving three months' written notice.

The joint data controllers may terminate this agreement with any party if following an investigation through the dispute procedure (see below) it is found that the contributing data controller is in breach of the Agreement.

15.2 Variation

Any proposed changes to the parties involved in this Agreement, or to any of the clauses contained herein will require the signature of the parties.

15.3 Dispute Resolution

In the event of a dispute arising under this Agreement, authorised representatives of the parties will attempt to resolve the dispute within ten working days of being requested in writing by any party to do so. If the dispute remains unsolved, it will then be referred to the DCR Programme Board who will use all reasonable endeavours to resolve the dispute within a further fourteen working days.

In the event of failure to resolve the dispute through the steps set out above the parties agree to attempt to settle it by mediation by a third party to be agreed.

If the dispute is in respect of the behaviour of a contributing data controller or a user(s) within that organisation which may involve a breach of data protection legislation, the joint controllers reserve the right to suspend access to the DCR for those user(s) or an entire organisation, pending an investigation of the suspected breach.

15.4 Resolution of Disputes with Data Subjects or the Supervisory Authority

In the event of a dispute or claim brought by a data subject or the Information Commissioner concerning the processing of shared personal data against either or both parties, the parties will inform each other about any such disputes or claims and will co-operate with a view to settling them amicably in a timely fashion.

The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the Information Commissioner. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

Each party will abide by a decision of a competent court in the UK or of the Information Commissioner.

16 CHANGES TO THE APPLICABLE LAW

If during the term, the data protection legislation changes in a way that the agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the parties will negotiate in good faith to review the agreement in the light of the new legislation.

APPENDIX 1

Parties to the Agreement

(1) **Dorset Council** of County Hall, Colliton Park, Dorchester DT1 1XJ;

(2) **Bournemouth, Poole and Christchurch Council** of Town Hall, Bourne Avenue, Bournemouth, BH2 6DY;

(3) **Dorset HealthCare University NHS Foundation Trust** of Sentinel House, Nuffield Industrial Estate, Nuffield Road, Poole BH17 ORB;

(4) **University Hospitals Dorset NHS Foundation Trust** of Longfleet Road, Poole, Dorset, BH15 2JB;

(5) **Dorset County Hospital NHS Foundation Trust** of Williams Avenue, Dorchester, Dorset DT1 2JY;

(6) **NHS Dorset Integrated Care Board** of Vespasian House, Barrack Road, Dorchester, Dorset, DT1 1TG; and

(7) **GP Practices in Dorset.**