Information Commissioner's Office

Dorset Care Record

Data Protection Impact Assessment – Dorset Care Record Version 2 (DCRv2)

This template is for you to record your DPIA process and outcome. The template follows the process set out in the Data Protection Impact Assessments (DPIAs) | ICO.

You should start to fill out the template at the **start** of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA

Identify the need for a DPIA. You may find it helpful to refer or link to other documents, such as a project proposal. Click here for guidance on this section.

1.1. Explain broadly what your project aims to achieve and what type of processing it involves.

The project aims to replace Dorset's existing shared care record Dorset Care Record Version 1 (DCRv1) with a new version Dorset Care Record Version 2 (DCRv2) that is based on an Interweave Digital platform. This DPIA relates to the first phase of the transition to the Interweave platform which replicates the existing DCRv1 with the scope limited to the ingestion and display of broadly the same information.

Any changes to the current system's processing and use of information will be detailed in this document.

The current shared care record has been operating since March 2018 and the driver for this change is the approaching end of contract with the current supplier. The expected date for transferring to the new platform is March 2026.

Each health and social care organisation holds its own set of records about individuals. These records may already be shared, through paper records, email or phone, when requested. A shared care record is a safe and secure way of bringing all these separate records from different health and care organisations together digitally in one place. It joins up information based on the individual rather than the organisation.

The DCR is a local health and social care record which brings together information from participating organisations. It is a copy of health and care information held by the participating organisations and is a key component of the data sharing requirements of the Dorset Integrated Care System (ICS).

The DCR holds data for patients who are registered with a General Practice in the Dorset ICS and also for people who have received treatment from any organisation that contributes data to the DCR where they have an NHS number.

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

The DCR is a business-critical system delivering the following benefits for the system:

- Non-cash releasing time savings
- Ability for patients to stay independent for longer and receive care and support in their homes or as close to them as possible
- Delayed need for long term care and unnecessary hospital admissions
- Better coordination of care for patients and their carers
- Reduced duplication and unnecessary visits
- Better management of medicines for the patient

The DCR is also in the business continuity plan for University Hospitals Dorset NHS Foundation Trust (UHD) in the event of an Electronic Patient Record (EPR) failure.

By moving to a new platform, there will be no change to the benefits for patients and staff involved in their care initially, during the first phase, as focus will be on replicating the data that is in DCRv1 and the experience for staff.

Information is only shared when it is needed to make direct care and treatment safer and more efficient. This helps to provide seamless integrated care and fulfil obligations under the Care Act 2016. Information is ‘view only’ in the patient record containing health and social care data from all source systems.

The organisations who contribute data to the DCR decide what personal information is collected and how it is used by the DCR. They are known as joint controllers under data protection legislation. The DCR joint controllers are:

- Dorset NHS Integrated Care System
- Dorset County Hospital (DCH)
- University Hospitals Dorset (UHD)
- Dorset HealthCare (DHC)
- Dorset Council (DC)
- Bournemouth, Christchurch and Poole Council (BCP)
- Dorset Primary Care practices
- Lewis Manning Hospice Care
- Weldmar Hospice Care
- Ringwood Medical Practice
- Coastal Medical Partnership.

1.2. Summarise why you identified the need for a DPIA.

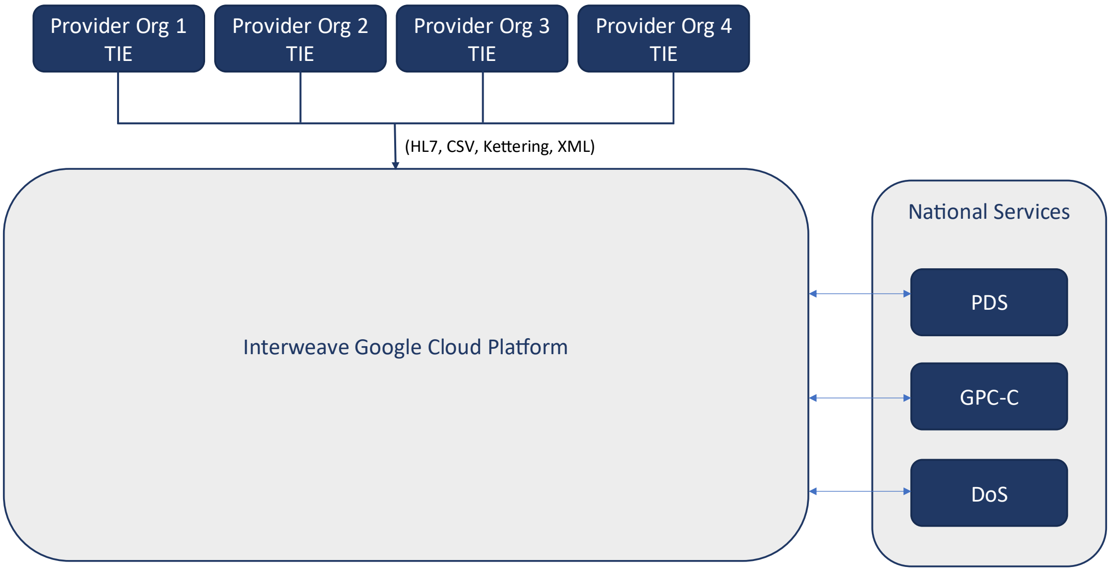
A DPIA is required because of the proposed changes to the storage and processing of data involving a large scale of health and social care data. This will ensure compliance with data protection legislation and ensure all risks are assessed and mitigated.

Step 2: Describe the processing

Describe the nature of the processing. You might find it useful to refer to a flow diagram or other way of describing data flows. Click here for guidance on this section.

2.1. How will you collect, use, store and delete data?

See below a high-level architecture diagram of the ingestion, processing and storage of data subject information.



DCR joint controllers (data controllers for the source systems) collate pre-determined data sets which are transferred electronically via their integration engines to a Dorset integration engine hosted by Interweave on Google Cloud Platform. The data will be transformed into Fast Healthcare Interoperability Resources (FHIR) stores (the global industry standard for passing healthcare data between systems) and stored on the Interweave Exchange. The DCR uses Virtual Private Networks (VPNs) which are encrypted connections to ensure protection of the data as it is ingested from existing partner systems.

If a message from a source system does not have a valid NHS number (and cannot be found following a look-up to the national Personal Demographics Service (PDS) when the message is received by the Dorset integration engine), the message will be stored and repeated attempts will be made to locate the NHS number in overnight batch jobs. However, messages without a valid NHS number will not be displayed in DCRv2.

Community data from DHC is called when a DCR user requests access to a patient's record using a Hypertext Markup Language (HTML) viewer connecting to TPP SystmOne, the electronic health record used by Community Services in Dorset. This data is not copied or stored in DCR. This technology is also used for providing Lewis Manning Hospice Care and Weldmar Hospice Care information and will also provide Oakhaven Hospice information in the near future

Primary care data is called when a DCR user requests access to a patient's record using a Hypertext Markup Language (HTML) viewer via GP connect to access the electronic health record used by Primary Care practices in Dorset. This data is not copied or stored in DCR.

Some end users will be able to access the DCR from their source systems through patient context launch. This will mean they can go directly from the specific patient record in their source system to the specific patient record in the DCR avoiding the need to sign-in and search for the correct patient. This reduces the likelihood of selecting an incorrect patient. It should be noted that the NHS number is encrypted in DCRv1 but will not be in DCRv2. This introduces a very low risk that staff could access another patient's record via the DCRv2 URL with a different NHS number. This risk is very low as the URL is not visible to the end user as a restricted pop-up window is used that does not display the URL.

The data will only be used for the provision of direct care. The DCR is a read only system therefore users cannot make any amendments to the data. The organisations who have access to the DCR are:

- Avon and Wiltshire Mental Health Partnership NHS Trust
- Bournemouth, Poole and Christchurch Council
- CHEC NHS Ophthalmologists
- Child Health Information Services (CHIS)
- Coastal Medical Partnership
- Community Pharmacies in Dorset
- Dorset Council
- Dorset Couty Hospital
- Dorset & Wiltshire Fire & Rescue Safe and Well Team
- Dorset Primary Care Practices
- Dorset HealthCare
- Dorset Integrated Care Board
- Harbour Hospital (part of Circle Health Group)
- Help & Care
- Julia's House Hospice
- Lewis-Manning Hospice Care
- Marie Curie
- Nuffield Health
- Oakhaven Hospice
- Reach
- Ringwood Medical Centre
- Salisbury NHS Foundation Trust
- Southern Health NHS Foundation Trust
- Special Care Dentistry (Dorset), Somerset NHS Foundation Trust
- Tricuro
- University Hospitals Dorset
- We Are With You
- Weldmar Hospice Care
- Wessex Cancer Alliance (part of University Hospitals Southampton)
- Wessex Clinical Van (part of Midlands Partnership NHS Foundation Trust)

- Yeovil Hospital

Data is only deleted from the DCR if a request to do so is sent from the source system, otherwise the data will remain in the DCR until it has reached the end of its retention period in line with the retention policy. The data deletion is “soft delete” and will keep the history of the resource available along with audit event for the deletion that took place.

The data will be shared with Interweave Digital, the suppliers of the system but will only be accessed by them for strictly limited purposes, such as for investigating and correcting errors and incidents.

In addition, Synernetics, a service provider who are sub-contracted by Interweave Digital to provide services for Interweave and as part of this are a sub-processor. They will be providing 2nd (application) and 3rd (infrastructure) line support. They are contracted via the NHS Standard Contract which contains a full Data Processing Agreement. They also have a “Standards Exceeded” DSPT, for extra assurance.

It will also be shared within the DCR and therefore will be accessible by the current user base. Users are only granted access if they are employed by an organisation which meets the onboarding requirements and complies with the conditions laid out in the Data Sharing Agreement.

Shared Care Records have been in place for several years and the technology for processing data in this way is tried and tested. Appropriate technical measures are in place and access to the DCR is monitored and audited with appropriate agreements in place. The processing is therefore not considered to be high risk.

Interweave is a mature shared care record dating back to 2018. It is the brand name of a shared care record solution in use across seven Integrated Care Systems (including Dorset).

Step 2.1: Describe the scope of the processing.

2.1.1. What is the nature of the data, and does it include special category or criminal offence data?

The following personal information is currently collected and shared (by the partners and PDS spine):

- identity details – name, gender, date of birth, NHS number;
- contact details – address, telephone, email address.

The UK General Data Protection Regulation (UK GDPR) gives extra protection to more sensitive information known as ‘special category data’. Information concerning health and social care falls into this category and needs to be treated with greater care. The information we share which falls into this category includes:

- details about health, treatment and care;
- data which may reveal racial or ethnic origin;
- data which may reveal religious beliefs;
- data which may reveal sexual orientation.

Patients whose PDS spine record are flagged as ‘sensitive’ will not be displayed in DCRv2 which will reduce the risk associated with displaying their records.

No criminal offence data will be included.

Across Dorset there is a population of approximately 800,000 people who can access health and social care services in addition to significant numbers of non-Dorset residents eg holiday makers. Some information regarding their health and social care will be shared with the DCR. Data is shared on a daily basis, sometimes several times each day.

The specific data sets collected (or viewed) are:

- Demographic information
- Alerts
- Allergies
- Encounters
- Appointments
- Documents
- Pathology results
- Radiology results
- Referrals
- Medicines
- Primary Care*
- Community Care

*If the technology is available at the point of implementation, primary care records will also include the records of deceased patients for 28 days after date of death.

The DCR has a Retention Policy which reflects the guidance set out in the NHS Records Management Code of Practice but does not have a retention solution with the current supplier. After the initial launch of the Interweave solution, work will be undertaken to ensure processes are in place to meet the requirements of the policy.

The DCR holds data for registered patients of a General Practice in the Dorset ICS and also for patients who have received treatment from any organisation that contributes data to the DCR where an NHS number is available.

Step 2.2: Describe the context of the processing.

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?
4. Do they include children or other vulnerable groups?
5. Are there prior concerns over this type of processing or security flaws?
6. Is it novel in any way?
7. What is the current state of technology in this area?
8. Are there any current issues of public concern that you should factor in?
9. Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

All health and care professionals accessing information in the DCR are required to have a legitimate relationship with the patient whose information they are accessing, i.e. they are directly responsible for providing health or social care for that patient. This includes children's data and that of other vulnerable groups.

A patient is able to opt out of the system at any time. While their data will be collected and stored in the DCR, it will not appear in any search and their information is beyond use. They can change their mind at any time and opt back in.

A patient can control whether their Primary Care record appears in the DCR, by opting out through their GP but cannot control what information from other partner source systems is available in DCR. If they choose to have a record in the DCR, then all information from other partner sources will be available according to services they have accessed, and what data sets have been agreed by each partner to be shared to the DCR.

If the technology is available at the point of implementing the Interweave platform, access to primary care records will also include the records of deceased patients for 28 days after date of death. The DCR DPO took advice from NHS England about providing access to deceased patients' records for coroners reports audit purposes and their view was that '*while the purpose of DCR is for the provision of direct care, it seems pedantic to access this information from individual source systems, when they could access it all from one place (and so speed up their processes)*'.

Patients generally expect their information to be shared between health care professionals who are responsible for their care. Many shared health records exist across the country however the DCR extends a shared health record into a shared health and social care record. The sharing of health and social care data has been public policy for a number of years at least since the first Caldicott report in 1997. The DCR formalises local data sharing agreements and provides a more secure environment for the sharing of this data.

The DCR programme engaged widely with the population of Dorset when the shared care record went live in 2018. A general leaflet drop was completed to all households prior to implementation of the changes from a consent model in early 2019 and there is a dedicated website containing information for the public about the DCR and the Privacy Notice. There is also further information about sharing information across health and social care organisations in the Dorset Integrated Care System (ICS) on the Our Dorset website.

Information shared to the DCR is secure with auditing capabilities and random audits are carried out regularly. The DCR programme will not make information available to any marketing or commercial company and is only available for the provision of direct care and with strict access criteria.

The Dorset Care Record has been live since 2018, however shared care records have been in existence in some areas for 20 years. Every ICS in England is required to have one and different shared care records are at different levels of maturity. There are no prior concerns over this type of processing

Any issues with public concern around the implementation of the Dorset Care Record were mitigated by communications to the public in 2019. This was via a leaflet drop and also the availability of leaflets and posters within places such as GP surgeries and libraries. Patients are also given the opportunity to opt out of the DCR and coupled with this, if a patient decided to opt out of the DCR they also have the opportunity to opt back in if they change their mind. No additional patient communications are planned as part of the transition to the new platform.

Interweave holds a “Standards Met” DSPT submission for the year 2024/25. Interweave also holds Cyber Essentials accreditation (Cyber Essentials: Certificate No: dc41c9fe-585d-4446-a481-68071b26c5de and Cyber Essentials PLUS : 1b3462a2-76e9-4763-9466-d4526809b88b).

Data is stored in the cloud in a fully encrypted environment. All messaging is encrypted and there is a security incident management in place which is in line with NIST guidance. The solution is compliant with ISO27001, 27017, 2018 and 27701 privacy standards.

Step 2.3: Describe the purposes of the processing.

1. What do you want to achieve?
2. What is the intended effect on individuals?
3. What are the benefits of the processing – for you, and more broadly?

The DCR benefits both health and social care organisations and patients by:

- Enabling patients to stay independent for longer, receiving care and support in their homes or as close to them as possible.
- Delaying the need for long term care and unnecessary hospital admissions.
- Offering an improved health and social care outcome for patients.
- Providing a seamless high-quality service.
- Fulfilling obligations under the Care Act 2016.
- Making direct care and treatment easier and faster. For example, this could include allowing a hospital doctor to see the medication that a GP has prescribed for a patient or allowing a GP to see what care, tests and treatment the patient received in hospital
- Providing better coordination of care for the patient and their care in the community, enhancing communication to avoid wasted visits and allowing better medicines management.

The key outcome for the programme is to make available a record of a patient's health and care to ensure that they can receive more timely treatment and support that is right for their needs. It will enable professionals across the health and care sector to work better and be more integrated by providing up to date and more accurate information. It will be safer for the patient and help to reduce unnecessary emergency pressures on the health system. The patient will also be able to rely on the fact that their information is readily available, secure and they do not have to keep repeating it, which may prevent incorrect information being provided and avoid mistakes. The update to this DPIA highlights the change in system platform to interweave with continuity at this stage being the required outcome.

Step 3: Consultation Process

Consider how to consult with relevant stakeholders. Click here for guidance on this section.

1. Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.
2. Who else do you need to involve within your organisation?
3. Do you need to ask your processors to assist?

Do you plan to consult information security experts, or any other experts?

Extensive work has been undertaken to identify the stakeholders that are likely to be impacted by this programme such as front-line health and social care staff, clinicians and consultants, GPs and support staff.

Broadly, stakeholders have been identified as:

- Joint controller organisations and their stakeholders (data contributors);
- Consumer organisations and their stakeholders; and
- NHS Dorset Integrated Care Board

Specific roles and the communication strategy for each role can be found in the communications plan.

A variety of communications routes will be utilised including:

- The staff website for current users of the DCR
- Support Channels – DCR contact number, email inboxes, meetings
- Emails & Newsletters – Regular updates to keep stakeholders informed of progress, milestones and next steps
- Governance meetings – Oversight of development and decision making
- On-line and in person familiarization sessions

The Information Commissioner's Office was also consulted and engaged with the project team to provide advice regarding the mitigation of risks to data.

The Data Protection Officer (DPO) and Cyber Security Lead for DCR have been involved in the project with engagement maintained via email and meetings as appropriate. Consultation was maintained through the development of the conceptual design and approval to proceed was received.

No changes are required to the privacy notice for the transition.

Feedback to the DPIA updates will be provided by the Pan Dorset IG Group.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures. Click here for guidance on this section.

Describe compliance and proportionality measures, in particular:

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

Data Protection legislation

To process personal data and special category data, a valid lawful basis must be identified from Article 6 and Article 9 of the UK General Data Protection Regulation (UK GDPR), respectively. The lawful bases which will be relied on for processing data for the DCR are:

6(1)(e) '...*the performance of a task carried out in the public interest or in the exercise of official authority...*'

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

With specific regard to safeguarding, in addition to Data Protection legislation 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.

9(2)(b) '...*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...'*

Common Law Duty of Confidentiality

For common law purposes, sharing information in DCR is based on implied consent. This is based upon the individual's "reasonable expectations" about how their data will be used and relies upon them knowing and understanding that ShCRs exist and gives health and care professionals the ability to access information about them.

"Reasonable expectations" can be viewed in the context of the "Caldicott 2" report;

> '*People ... expect professionals to share information with other members of the care team, who need to co-operate to provide a seamless, integrated service*'.

Also;

> *'There is in effect an unwritten agreement between the individual and the professionals who provide the care that allows … sharing to take place. This requires the health and social care professional to treat the patient on the basis of their needs and keep the patient's information confidential. In return, the health and social care professional is able to rely on 'implied consent' when sharing personal confidential data in the interests of direct care, as long as the patient does not object, or has not already done so'.*

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 applies 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.

Any changes to the information sharing principles will be made available to patients via the dedicated website, the DCR Privacy Notice and information sharing strategies across Dorset ICS published on the Our Dorset website.

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 UK General Data Protection Regulation (GDPR) 2019.

There is little scope for function creep as use of the DCR is only for the provision of direct care. The DCR programme has strong pan partner governance in place using standard project management methods to manage implementation and prevent function creep. Without the DCR, the information is still available to professionals through existing means such as email, letter and telephone or giving access to other systems. However, this is costly, time consuming, less secure and open to error and duplication which can slow provision of care.

Contractual and security arrangements are in place to ensure the data does not leave the European Union.

All users of the DCR will/have received mandatory training on security and information sharing. Users will not be given logon details and access to the system until they have completed the required training and achieved a certificate of assessment. This allows the DCR to be able to audit the level of the understanding and ensure that patients' right to privacy are of upmost importance.

Other measures to support compliance and protection of privacy are:

- Data Sharing Agreements signed by all organisations accessing the DCR.
- A Privacy Notice, leaflets and literature available on the website providing details about patients' rights and assurance that they are supported.

- A dedicated Data Protection Officer to ensure patients' rights are protected at all times.
- A pan Dorset IG group represented by IG leads from partners to ensure a consistent approach to information sharing and privacy across Dorset. A key role of this group is ensuring best practice and compliance with data protection legislation and appropriate data sharing

All activity is auditable and a list of any organisations accessing their record is available to patients under a subject access request. A data subject requesting a copy of their records will be referred to the source organisation.

Interweave have a variety of security measures in place to ensure that the data is protected once it is available within the DCR. They have relevant approved codes of conduct/security certifications in place and have Security Officers and Data Protection Officers within their organisation. The DCR team ensure that the security matrix is kept up to date with every addition of new data.

Step 5: Identify and assess risks (see Appendix A)

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.		**Likelihood of harm**	**Severity of harm**	**Overall risk**
Risk		Score	Score	Score
1.	Professionals could access a patient's record where they do not have a legitimate relationship with the patient.	Possible	Serious	Significant
2.	Some patients may not be aware that they have a record in the DCR	Likely	Serious	Significant
3.	Some patients may object to their health and social care information being combined into one record	Likely	Serious	Significant
4.	System could be compromised	Unlikely	Major	Significant
5.	Loss or inadequacy or corruption of data	Unlikely	Major	Significant

Step 6: Identify measures to reduce risk (see Appendix A)

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Score	Yes/no
1. Professionals could access a patient's record where they do not have a legitimate relationship with the patient	• DCR Partners are required to comply with information governance legislation. • Mandatory Training and assessment by all; prior to access given • All partners sign a Data Sharing Agreement • Access is auditable and abuse of use of DCR will result in removal of access and can be a disciplinary offence • Legal partnering agreement detailing partner accountabilities • Before accessing a patient's record, the Interweave platform requires staff to confirm they have a legitimate relationship with the patient. • Staff will not be able to circumnavigate access by editing the patient context launch URL with a different NHS number as the URL will not be visible.	Reduced	Low	Yes

2. Some patients may not be aware that they have a record in the DCR	• Robust communications campaign or the public ensuring best endeavours to wide public groups including extensive engagement with vulnerable and minority groups. • Opt out process that is easy for individuals to understand and action. • Widely distributed information • Wide availability of communication and resources, literature allowing individuals easy access to communicate their wishes reducing the risk of access without knowledge or permission. • Robust training programme to inform clinicians re use of the data • Robust governance developed to review requests for data. • Dedicated website providing a variety of information regarding the DCR	Reduced	Low	Yes
3. Some patients may object to their health and social care information being combined into one record	• Robust communications campaign or the public ensuring best endeavours to wide public groups including extensive engagement with vulnerable and minority groups. • Opt out process that is easy for patients to understand and action. • Widely distributed information • Wide availability of communication and resources, literature allowing patients easy access to communicate their wishes reducing the risk of access without knowledge or permission. • Robust training programme to inform clinicians re use of the data • Robust governance developed to review requests for data. Dedicated website providing a variety of information regarding the DCR	Reduced	Low	Yes

4. System could be compromised	• Centralised System Admin role to manage data quality. Data quality group monitor and take accountability. Robust technical testing process. • Robust penetration testing practice using external supplier – ethical hackers • Robust internal testing strategy and procedures before any data becomes live • BC/DR policy in place	Reduced	Medium	Yes
5. Loss or inadequacy or corruption of data	• Centralised System Admin role to manage data quality. Data quality group monitor and take accountability. Robust technical testing process. • Robust penetration testing practice using external supplier – ethical hackers • Robust internal testing strategy and procedures before any data becomes live • BC/DR policy in place	Reduced	Medium	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
1. DPIA submitted to DPO:	26/02/2025	DPIA reviewed by DPO and referred to Pan Dorset IG Group
Summary of DPO advice:		
2. Date referred to Pan Dorset IG Group	12/08/2025	
Summary of Pan Dorset IG Group advice:		
3. Residual risks approved by:	N/A	If accepting any residual high risk, consult the ICO before going ahead
Comments:		
4. This DPIA will kept under review by:	DCR Project Manager	The DPO should also review ongoing compliance with DPIA
Comments:		
5. DPIA approved by DPO	09/09/2025	

Appendix A

Risk Matrix	**Likelihood**				
Severity	**1 Rare**	**2 Unlikely**	**3 Possible**	**4 Likely**	**5 Almost Certain**
5 Catastrophic	5	10	15	20	25
4 Major	4	8	12	16	20
3 Serious	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Negligible	1	2	3	4	5

Key to Risk Register rating:

Low Risk Green 0-3	Moderate Risk Yellow 4-6	Significant Risk Orange 8-12	High Risk Red 15-25

RISK ASSESSMENT: [using the matrix above]			
INITIAL risk rating – step 5 (before any mitigating actions have been implemented)	Severity (example) 4	Likelihood (example) 4	Total (example) 16
CURRENT risk rating – step 6 (at time of writing, taking account of existing controls and mitigating actions)	Severity (example) 3	Likelihood (example) 4	Total (example) 12