Data Protection Impact Assessment (DPIA) – Dorset Care Record

---

This template is for you to record your DPIA process and outcome. Guidance on how to complete this DPIA can be found in the CCG Data Protection and Security policy. The template follows the process set out in the ICO DPIA guidance.

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

1. Explain broadly what project aims to achieve and what type of processing it involves.
2. You may find it helpful to refer or link to other documents, such as a project proposal.
3. Summarise why you identified the need for a DPIA.

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 Dorset Care Record (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 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.

The DCR enables timely access to key information in the health and social care records of patients. 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.

By making more up to date information, more readily available to health and care practitioners, the DCR aims to realise the following benefits for Dorset's residents:

- 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

Access to the DCR is for the provision of direct care and information is only shared when it is needed to make 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 one complete record for the patient containing all health and social care data from all source systems.

The DCR partners are the organisations who 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 partners 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) and the GP practices in Dorset.

A DPIA is required as the processing involves 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. The DPIA was initially completed in the early stages of the project when the technical design was still being developed. This version has since been reviewed and refreshed to reflect changes in the system and data protection legislation.

Step 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?
2. What is the source of the data?
3. Will you be sharing data with anyone?
4. You might find it useful to refer to a flow diagram or other way of describing data flows.
5. What types of processing identified as likely high risk are involved?

Data from GP Practices is called when a DCR user requests access to their record using a Hypertext Markup Language (HTML) viewer connecting to TPP SystmOne, the electronic health record used by GP Practices in Dorset. This data is not copied or stored in DCR.

All other DCR partners (data controllers for the source systems) collate pre-determined data sets which are transferred electronically via their integration engines. This data is stored in the DCR data base provided by the system supplier, Orion Health and located within the Redcentric data center. and is protected by industry-standard firewalls with live, real-time 24/7 monitoring. 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.

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 GP 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 will be shared with Orion Health, 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. It will also be shared within the DCR and therefore will be accessible by all users. 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.

Describe the scope of the processing:

1. What is the nature of the data, and does it include special category or criminal offence data?
2. How much data will you be collecting and using?
3. How often?
4. How long will you keep it?
5. How many individuals are affected?
6. What geographical area does it cover?

The following personal information is currently collected and shared:

- 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.

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. Some information regarding their health and social care will be shared with the DCR. Visitors who access health and care organisations in Dorset may also have their data shared into the DCR. Data is shared on a daily basis, sometimes several times each day.

The DCR has a Retention Policy which reflects the guidance set out in the NHS Records Management Code of Practice and work is underway with Orion Health 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.

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 GP 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 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.

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 has engaged widely with the population of Dorset. 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. 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 can also have the opportunity to opt back in if they change their mind.

The system supplier, Orion Health, published a standards exceeded Data Security and Protection Toolkit for 2023/24. They have also adopted ISO 27001:2013 alongside their own internal information security policy. They also hold a BS 10012 certification as part of their compliance with the Data Protection Act 2018.

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 full 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.

Step 3: Consultation Process

Consider how to consult with relevant stakeholders:

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?
4. 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, support staff and patients, including minority groups.

A list of stakeholders identified as part of the original mapping process are below:

- Partner organisations and their stakeholders:
- Dorset Council, Bournemouth, Christchurch & Poole Council
- Dorset Integrated Care Board
- Dorset HealthCare
- University Hospitals Dorset and Dorset County Hospital

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

Other stakeholders

- Public Health Dorset
- Dorset Community Action
- Help the Aged
- Hospices – Weldmar, Julia's House, Poole Hospice
- Day centres and carers
- Councils – Districts, towns, parish
- Healthwatch Dorset
- Wessex Academic Health Science Network
- Healthcare Wessex
- Residents

Activities undertaken to consult and engage with stakeholders have included:-

- Roadshows
- Surgeries
- Presentations
- Workshops
- Newsletters
- Editorials
- Leaflets
- Markets and supermarket presence
- Website and social media

- Community groups
- Surveys and questionnaires
- Case studies
- Videos and blogs

Written information has also been made available in the three main other languages (Polish, Mandarin and Urdu) as well as Easy Read versions. Stakeholders such as People First Dorset have been instrumental in designing and developing alternative versions of media to support minority groups.

The original DPIA was approved by the Pan Dorset IG Group.

Step 4: Assess necessity and proportionality

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.

Information sharing principles will be made available to patients via the dedicated website, the DCR Privacy Notices 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 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 organis~~z~~ation.

Orion Health 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	Minimal	Low
2.	Some patients may not be aware that they have a record in the DCR	Probable	Significant	Medium
3.	Some patients may object to their health and social care information being combined into one record	Probable	Significant	Medium
4.	Some patients could receive multiple letters from different partners responsible for an aspect of their care which cause confusion	Probable	Significant	Medium
5.	System could be compromised	Possible	Severe	High
6.	Loss or inadequacy or corruption of data	Possible	Severe	High
7.				

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 users 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 • Communications and engagement plan to raise awareness of information security to employees and partner organisations	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. Some patients could receive multiple letters from different partners responsible for an aspect of their care which cause confusion	• Use of dedicated website and other publicly available information to keep messages current • Joint DPIA and associated policies scrutinised and owned by each partner and supported by the Pan Dorset IG Group • Agreed project management approach and governance arrangements in place • Pan Dorset IG group supporting information and advising on legal practice	Reduced	Low	Yes

5. 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
6. 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. Measures approved by:	Pan Dorset IG Group	Integrate actions back into project plan, with date and responsibility for completion
Summary of DPO advice:		
2. DPO Advice provided	Pan Dorset IG Group	Integrate actions back into project plan, with date and responsibility for completion
Summary of DPO advice:		
3. Residual risks approved by:	DCR Board	If accepting any residual high risk, consult the ICO before going ahead
Comments:		
4. This DPIA will kept under review by:	DCR Project Management Office	The DPO should also review ongoing compliance with DPIA
Comments: v2 updated to incorporate decommissioning of the DiSC and Discussion to review and to reflect current legislation.		

Version Control		
Date of issue	**Version No**	**Nature of change**
November 2021	1.1	Update to list of organisations with access to DCR
May 2023	1.2	Update to list of organisations with access to DCR
August 2023	1.3	Update to list of organisations with access to DCR
November 2023	1.4	Update to list of organisations with access to DCR
December 2023	1.5	Update to list of organisations with access to DCR
January 2024	1.6	Update to list of organisations with access to DCR
November 2024	1.7	Update to list of organisations with access to DCR
March 2025	2.0	Updated to reflect the decommissioning of the Dorset Information Sharing Charter and Discussion to View (as approved by the Pan Dorset IG Group and DCR Programme Board) and current data protection legislation
April 2025	2.1	Update to list of organisations with access to DCR