Data Protection Impact Assessment (DPIA) – MY DCR (CITIZEN PORTAL)

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The purpose of this DPIA is to outline the type and method of processing data, which is classed as personal and special categories, and may result in a high risk for individuals. We are introducing new technology to process data on a large scale across Dorset which may be directly accessed, used and updated by citizens alongside clinicians who support and provide care services. The Dorset Care Record (DCR) aims to integrate health and social care so that people, patients and carers only have to tell their story once. The DCR Clinical Portal is used by clinicians and professionals in a health and care setting. The original DPIA for the Dorset Care Record can be found here. We are now looking to explore and deliver the ambition for personal health records (PHR) as per the national context for online access to personal records for empowered self care. A personal health record (PHR) can be defined as follows: • it's secure, usable and online • it's managed by the person who the record is about and they can add information to their PHR • it stores information about that person's health, care and wellbeing • health and care sources can add information to the PHR Personal Health Records are sometimes called other things, like patient or citizen portals – the DCR portal will be called MY DCR. The DCR Citizen Portal draws information from the DCR Clinical Portal to provide the patient/citizen with a secure and limited view of their information held on DCR. The record will show the following: • Access to care summaries, such as discharge and visit summaries. • Access to condition-specific educational information. • Relationship management through circle of care. • Contribute to and set personal health goals through goals and actions.

- View past and future appointments across the care continuum.
- Secure file sharing between patients and clinicians.
- Patient-controlled email notifications for activities related to shared files, documents and appointments.
- View current and past lab results (limited availability).
- View current and past medications.

For the most part, information shown in My DCR will be view only and taken from the clinical portal. However, the citizen will be able to append some localised information such as adding to their circle of care and upload/share files with their clinician.

My DCR will enable the invitation to secure access to specialty pathways such as the maternity pathway and the cancer follow-up pathway (with the potential of more to follow). Patients/citizens will only be able to join these pathways through a secure invitation issued by their clinician via My DCR once a discussion has taken place.

All access and activity is fully tracked and audited using an agreed policy. Some pathway reports are accessible to the DCR Privacy Officer.

An Equality Impact Assessment has been approved and can be found here – EqIA (Citizen Portal)

The partnership programme is being supported by NHS Dorset Clinical Commissioning Group, Dorset County Hospital, University Hospitals Dorset NHS Foundation Trust (previously Poole Hospital Foundation Trust and Royal Bournemouth and Christchurch Hospital), Dorset HealthCare, Dorset Council, Bournemouth, Christchurch & Poole Council and the South Western Ambulance Trust and includes GP practices in Dorset.

The DCR has been developed within the framework of the Dorset Information Sharing Charter (DiSC), which aims to provide Dorset partner agencies with a robust foundation for the lawful, secure and confidential sharing of personal information. The Charter enables partner organisations to meet their statutory obligations and share information safely to enable integrated service provision across the county and better care outcome for its residents.

Information about DISC can be found at https://www.dorsetforyou.gov.uk/disc.

Step 2: Describe the processing

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

The nine key partners who together make 'the partnership' or 'the partners' of the DCR who provide source data and who data share in accordance with the data sharing agreement – are as follows:

- Dorset Clinical Commissioning Group (DCCG)
- The Four Foundation Trusts
    - Dorset County Hospital (DCH)

- University Hospitals Dorset NHS Foundation Trust (previously Poole Hospital Foundation Trust and Royal Bournemouth and Christchurch Hospital)
- Dorset HealthCare University Foundation Trust (DHC)
- South West Ambulance Services (SWAST)

- The two Local Authorities in Dorset
  - Dorset Council (DC)
  - Bournemouth, Christchurch and Poole (BCP)
- GP practices across Dorset

In addition, for My DCR and Pathways, supplementary data can be appended to the source data and shared (as mentioned above) by the following:

- Citizens/Patients in Dorset
- Circle of Care – family, friends, charities or whomever the citizen chooses to share their record with, in respect of their care

Clinicians working in services where a pathway exists will belong to a specific role (behind the scenes in DCR) to facilitate access to information and the ability to invite patients onto the pathway through the citizen portal to provide easy secure online access to support the delivery of better care in Dorset.

Data will be collected daily as a minimum from partner systems using secure interfaces which will feed/update the DCR clinical portal; this includes a view/instant retrieval of the GP record which matches the source record.

The DCR does not change the length of time that data is retained when received from partners and GPs.

However, any data added directly by the patient/individual may be added at any point during their care pathway and will be retained in accordance with existing retention policy (8 years = 7 years plus current year) upon closure of the record in the majority of cases.

If a patient requests for pathway data (ie data they have contributed to directly via the pathway) to be changed or removed, the request should be directed to the DCR Privacy Officer who will manage in accordance with the existing DCR Subject Access Request Standard Operating Procedure (SOP).

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
The DCR covers all persons accessing health and social care services in Dorset which equates to approximately 800,000 persons. It includes personal data (such as name, address and date of birth) as well as special category data about someone's health conditions and social care needs. The processing will be large scale and volume of data will be extensive as individual health records grow. The data will be collected in 'real time' on a daily basis. These will be managed in accordance with the DCR retention policies within the main DCR DPIA.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? 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 will have/required to have a legitimate relationship with the person whose information they are accessing, i.e. they are directly responsible for providing health or social care for that person. This will include children and vulnerable people. In some settings, patients will already have access to their data being held by that specific partner – a good example is access to the GP record held by the GP through the primary care provider portal. All patients/citizens will have legitimate access to their record via My DCR and/or pathways in a secure and trusted way. The core processing will be consistent for all data however, individuals will be able to exercise their right to rectify incorrect or absent data with the partner who provides/controls the source data. However, the right to rectify or absent data is not absolute within Health and Care records. Comments can be added to a record where a citizen does not agree with the clinical decisions and notes within a record.

When patients/citizens are enrolled on a pathway, they will have the ability to add to their core record and to upload documents which they feel provide suitable information to support their health and care needs. These documents will be visible to their care professionals.

The functionality to share their record with a family members or carer via their circle of care will exist for the patient and it will be their choice as to whether they choose to use this functionality or not (the option to revoke access also sits with the patient). There is also the ability for clinicians to revoke access for patients that are identified as vulnerable.

A patient/citizen can choose to opt out of the patient portal. However, they can change their mind at any time and opt back in by contacting the Privacy Officer. This will be recorded in the audit trail.

A Privacy Notice is available to all through the DCR website.

Partners agree that the communications and engagement campaign with the public, including vulnerable and minority groups has been extensive and reasonable considering the demographics of the county.

Information shared to the DCR is secure with auditing capabilities. **The DCR programme <u>will not</u> make the information available to any marketing or commercial company. Currently data <u>is only</u> available for direct care and with strict access criteria. The data is not currently to be used for secondary use purposes. Any future decisions on the use of DCR data for secondary purposes will require consultation and board approval. Citizens will retain the right to exercise their National Data Opt Out rights.**

All partners have signed the DiSC which ensures a consistent and robust approach to information sharing via agreed principles.

As the DCR is hosted by the Dorset Council, compliance with the Public Services Network Connection Compliance Certificate (PSN CoCo) is secured and renewed annually along with the annual submission of the NHS Digital Data Security and Protection Toolkit.

In addition, periodic audits and reviews are conducted, with the most recent Penetration Testing and Cyber Review taking place in October 2021.

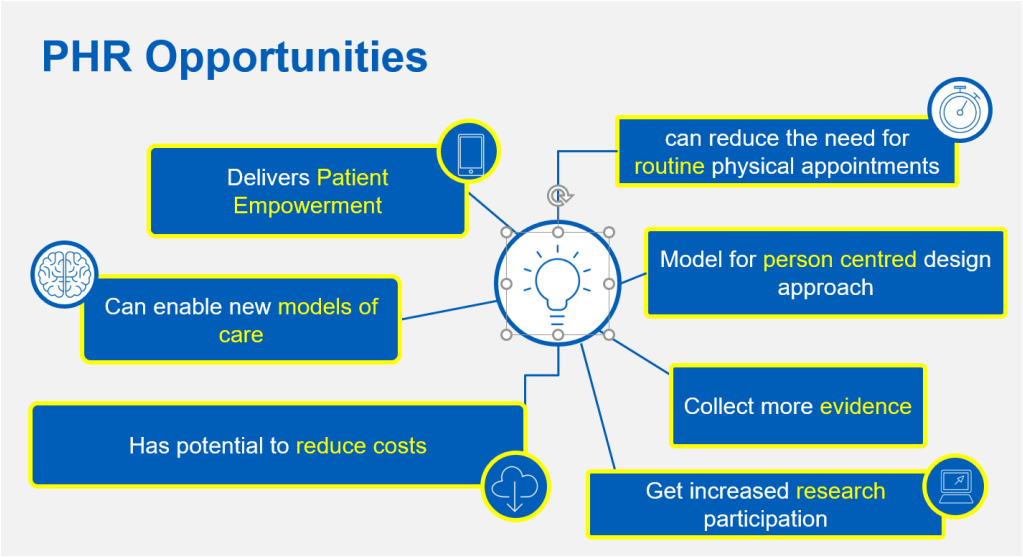
Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The DCR Citizen Portal and Pathways will deliver future opportunities and benefits to all stakeholders, as summarised below.

Citizen Portal

- Better coordination of care around the person and their carer
- Reduced duplication and unnecessary visits
- Citizen choice, control and empowerment
- Access to information at a time and way to suit the individual

Below is a summary taken from the NHS Digital PHR Programme and further helpful/useful information and guidance can be found here:



The changes to processing and providing citizens with access to their records will not be without challenges and some are summarised below:

Clinical engagement and buy-in – cultural shift

Vendor lock-in and interoperability between systems and solutions

Standards for the overarching Personal Health Record (delivered by My DCR and/or Pathways)

Sustainable business case

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? 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, support staff and all citizens, including minority groups. A stakeholder mapping exercise has been undertaken and is reviewed regularly as the programme progresses through incremental implementation. A communications and engagement strategy is in place and continually reviewed and developed through the phases of implementation.

Dedicated officers within the programme supported by partner colleagues ensure the strategy and actions plans are delivered and evaluated to ensure as wide engagement as possible. It is however not possible to engage with all groups all of the time. Engagement is prioritised based upon the highest impact or interest at particular points in the implementation timeline and availability of the system.

A list of stakeholders identified as part of this mapping process are below:-

Partnership organisations and their stakeholders
Dorset Council (DC), Bournemouth, Christchurch & Poole Council (BCP) and third party organisations

- Members including Cabinet and Full Council and portfolio holders and committees
- Safeguarding Board (DC)

Dorset Clinical Commissioning Group (DCCG)

- Patient Engagement Group (PEG)
- Patient Participation groups (PPGs)

Dorset Healthcare

- Community hospitals – Shaftesbury, Blandford, Bridport, Weymouth, Swanage, Wareham, St Leonards, Wimborne, Westhaven and Sherborne
- Community based services – health visitors, district nurses, community matrons
- Mental health services
- Patients and patient reference groups
- Governors
- Non-executive boards
- PALS

University Hospitals Dorset (Royal Christchurch and Bournemouth Hospitals, Poole Hospital) and Dorset County Hospital

- Acute services
- Boundary hospitals
- IT and Third parties
- Governors
- Friends of…
- Non-executive boards
- Patient reference groups
- Patient advice and information liaison service (PALS)
- Consultants
- WRVS
- Nursing teams
- Hospital based social care teams
- Pharmacies
- Patients

South Western Ambulance Services Trust (SWAST)

- Paramedics
- Auxiliaries

Other Stakeholders

- Public Health Dorset
- Dorset Community Action
- Help the Aged
- Hospices – Weldmar, Julia's House, Poole Hospice
- Day Centres and carers

- Councils – district, town, parish
- Dorset Race Equality Council
- Healthwatch Dorset
- Wessex Academic Health Science Network
- Wessex Care Record - LHCR
- Healthcare Wessex
- Residents
- Her Majesty Prisons - Verne, Portland and Guys Marsh

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

Evidence of activities already undertaken can be provided on request. Written information has been also 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.
Engagement with the ICO Public Engagement team has been extremely constructive and helped inform the changes to the system to move from use of consent to public task as the legal basis for information sharing.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The primary consideration of the DCR programme is to improve the quality of health and social care whilst maintaining the highest levels of confidentiality.

Health and Social Care Act 2012

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

Section 251 NHS Act 2006 – provides a basis, through regulations, for setting the common law confidentiality requirements aside, generally replacing them with approvals or other conditions.

The Human Rights Act (Article 8 of the European Convention on Human Rights) requires reasonable objections to the disclosure of personal confidential data to be respected.

Care Act 2014

The Care Act 2014 reforms the way the adult social care system works in England including how care is delivered. The aim of the Care Act 2014 is to bring together a number of separate pieces of health and social care legislation.

Changes implemented in 2015 included a range of new obligations for local authorities around the provision of information and advice, the integration of care and support with health-related services and eligibility assessments. It also strengthened the rights and recognition of carers in the social care system.

Common Law Duty of Confidence (the common law of confidentiality)

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

The DCR will allow sharing for direct care to become more reliable and systematic, but it will not change the legal basis of implied consent.

Implied consent to access relevant information about the patient, or to share it with those who provide (or support the provision of) direct care to the patient can be relied on as a legal basis if the following conditions are met:

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

The DCR meets the above conditions. In addition, a health and care professional will ask the individual whether they give consent for them to access the DCR at the point of care.

UK GDPR

Under UK GDPR there must be a valid lawful basis to process personal data. **For UK GDPR sharing information for the DCR is on the basis of public task** where "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

Article 6(1)(e) of the UK GDPR is the condition for lawfully processing data for delivering direct care as part of the DCR:

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

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

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

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

Safeguarding

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

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

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

The programme has strong governance in place across Dorset using standard project management methodology to manage the implementation and prevent function creep. Without the DCR, the information can still be available to professionals through existing means such as email, letter and telephone or giving access to other systems.

Contractual and security arrangements are in place to ensure the data is stored in the United Kingdom.

All users are trained which includes mandatory online learning 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 the person's rights to privacy are of upmost importance.

Other measures to support compliance and protection of privacy are:-

- Partners have signed the DiSC which ensures compliance to processing of information in a consistent and legal way.
- The Joint Data Controller agreement ensures shared accountability by partners and is a legal document.
- The Personal Information Sharing Agreements, Privacy Notice, leaflets and literature available on the website provides assurance to the person that we support their rights of privacy.
- A dedicated Privacy Officer will ensure the system is compliant and a subject's rights are protected at all times.
- Staff working directly on the project have signed confidentiality agreements and all partners have their own internal process for their staff to ensure policies and procedures on privacy and information sharing are followed.
- A pan Dorset IG Group is chaired by a Partner Organisation and represented by IG leads from all partners ensure a consistent approach to information sharing and privacy across Dorset as a partnership approach. Quality and best practice is a key role of this group.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
1. Professionals could access subject's record where they do not have a legitimate relationship with the subject.	Possible	Minimal	Low
2. Auditing and reporting functionality is not fit for purpose or readily available	Possible	Minimal	Low
3. Some subjects may not be aware that they have a DCR created and self service access to their record will be available via the Citizen Portal	Probable	Significant	Medium
4. Some subjects may object to their health and social care information being combined into one DCR record	Possible	Significant	Medium
5. System could be compromised – system timeout (if left logged in), portal logins shared, individuals do not protect their personal password and mobile technology (including using public computers and wifi)	Possible	Significant	High
6. Loss or inadequacy or inaccurate or corruption of data	Possible	Minimal	High
7. Personal and/or special category information is inappropriately shared by the citizen/patient or somebody with access via the Circle of Care (presenting a risk to a vulnerable adult or child)	Possible	Significant	Medium/ High
8. Authentication of the individual for secure access to the portal and possible pathways – to ensure data and communication is with the right person (dependency on national NHS tools such as NHS Login and supplier solution security)	Possible	Minimal	Medium

Step 6: Identify measures to reduce risk

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** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved** Yes/no
1. Some subjects may not be aware that they have a DCR created 2. Some subjects may object to their health and social care information being combined into one record	- Robust communications campaign to the public ensuring best endeavours to wide public groups which includes extensive engagement with vulnerable and minority groups. - Opt out process that is easy for individuals to understand and action. - Widely distributed information - Leaflets and forms. - Centralised Privacy Management to manage opt out and other aspects. - Wide availability of communication and resources, literature will allow individuals easy access to communicate their wishes which will reduce the risk of access without knowledge or permission. - Training of staff should ensure that the patient is content for them to view their shared record at point of care with a record that a discussion has taken place. - Robust training programme to inform clinicians re use of the data - Robust governance developed to review requests for data. - Leaflet drop from partnership to all Dorset households stating legal	Reduced Reduced	Low Low	

	basis for sharing to DCR. Advise of data processing - Update appropriate documents such as PISA and Privacy notice and upload to website - Review and update all printed resources and website information - Comms leads in partners to deliver public awareness about what is health and what is social care – myth busting to help public become more aware. Also deliver training o staff to help educate the public			
xxxxxxxx 3. System could be compromised 4. Loss or inadequacy or inaccurate or corruption of data	- Centralised System Admin role to manage data quality. Data quality group to monitor and take accountability. Robust technical testing process. - Monthly review of the system with Orion Health - Monthly scans and patching windows of the system with Orion Health - Once the system is up and running there will be regular penetration testing - Citizen Portal logins will be personalised to individuals and guidance/good practice shared at the time of issue - System/Portal timeout in place and will disconnect after 10 minutes if left logged in without any activity - DCR safeguards in place to protect any data loss/gathering via public computers and/or public wifi	Reduced Reduced	Medium Medium	

	- Robust penetration testing practice using external supplier – ethical hackers completed in October 2021 - Robust internal testing strategy and procedures before any data becomes live - Business Continuity and Disaster Recovery plan in place			
5. Personal and/or special category information is inappropriately shared by the patient or somebody with access via the Circle of Care	- Clinicians to invite patient and outline mutual responsibilities - Clear supporting literature/guidance to be provided to patient - Simple method to revoke or remove people previously added to Circle of Care/Shared access to record	Reduced	Medium	
6. Authentication of individual for secure access to the portal and possible pathways – to ensure data and communication is with the right person	- Partners to ascertain identity of the patient when invitation to join is generated by the clinician (e.g. 3 point check) - creation and periodic use of the security questions upon login by the patient - if an account is not accessed within a defined period it becomes locked - all accounts will use a strong password enforced by the software - delivered in accordance with the requirements of the NHS Data Protection and Security Toolkit	Reduced	Medium	

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	*e.g - Pan Dorset IG Group*	*e.g Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:	*e.g. - DCR Board*	*e.g. If accepting any residual high risk, consult the ICO before going ahead*
DPO advice provided:	*e.g Pan Dorset IG Group* *Partner DPOs* *ICO Public Engagement Team*	*e.g. DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		*If your decision departs from individuals' views, you must explain your reasons*
Comments:		
This DPIA will kept under review by:	Pan Dorset IG Group	*e.g The DPO should also review ongoing compliance with DPIA*