Data Protection Impact Assessment (DPIA) Template

A DPIA is designed to describe your processing and to help manage any potential harm to individuals' in the use of their information. DPIAs are also important tools for demonstrating accountability, as they help you as a Controller to comply with the requirements of the Data Protection Legislation. Non-compliance with DPIA requirements can lead to fines imposed by the Information Commissioners Office (ICO); this includes not carrying out a DPIA at all, carrying out a DPIA in an incorrect way or failing to consult the ICO where required.

DPIA's are not new; the use of Privacy Impact Assessments has become common practice in the NHS and can provide evidence of compliance within the Data Security and Protection toolkit (DSPT); DPIAs build on that practice.

It is not always clear whether you should do a DPIA or not but there are a number of situations where a DPIA **should** be considered or where a DPIA is a **legal requirement**. If you can tick against the criteria below it is highly recommended that you undertake a DPIA and if you decide not to, ensure that you document the reasons for your decision.

You as Controller **MUST** carry out a DPIA where you plan to:	Tick or leave blank
Use **profiling or automated decision-making** to make significant decisions about people or their access to a service, opportunity or benefit;	☐
Process **special-category data or criminal-offence data on a large scale**;	✓
Monitor a publicly accessible place on a large scale;	☐
Use **innovative technology** in combination with any of the criteria in the European guidelines;	☐
Carry out **profiling** on a large scale;	☐
Process biometric or genetic data in combination with any of the criteria in the European guidelines;	☐
Combine, compare or match data from multiple sources;	✓
Process personal data **without providing a privacy notice** directly to the individual in combination with any of the criteria in the European guidelines;	☐
Process personal data in a way that involves **tracking** individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;	☐
Process **children's** personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;	☐
Process personal data that could result in a **risk of physical harm** in the event of a security breach.	☐

You as Controller should **consider** carrying out a DPIA where you	Tick or leave blank
Plan any major project involving the use of personal data;	✓
Plan to do evaluation or scoring;	☐
Want to use systematic monitoring;	☐
Process sensitive data or data of a highly personal nature;	✓
Processing data on a large scale;	✓
Include data concerning vulnerable data subjects;	✓
Plan to use innovative technological or organisational solutions;	☐

A new DPIA should be carried out if you decide that there is a significant enough change to what you originally intended but it is good practice for DPIAs to be kept under review and revisited when necessary.

There is guidance to help you. Your Data Protection Officer (DPO) can be consulted before completing a DPIA in order to provide specialist advice and guidance or simply to talk things through with you.

Background Information	
Date of your DPIA :	13/10/2021
Title of the activity/processing:	Devon and Cornwall Care Record
Who is the person leading this work?	Clive Taylor, Project Manager Devon ICS Digital Transformation Team
Who is the Lead Organisation?	Devon ICS & Cornwall ICS
Who has prepared this DPIA?	Alex Bunn, Information Governance Consultant
Who is your Data Protection Officer (DPO)?	There are multiple Controllers whose DPOs will be consulted
Describe what you are proposing to do: (Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).	The programme aims to bring together care records pertaining to multiple Controllers into a 'shared record' that can be accessed either directly from individuals' records within the Controllers' own record system or through a web portal. The web portal will be internet based (so a HSCN connection is not required for access).
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is).	Yes –

Key contact	Organisation
Exemption 40 (2)	Cornwall Council
Exemption 40 (2)	Cornwall Partnership NHS Foundation Trust
Exemption 40 (2)	DAAT
Exemption 40 (2)	DELT Shared Services Ltd
Exemption 40 (2)	Devon Council
Exemption 40 (2)	Devon Docs
Exemption 40 (2)	Devon Partnership NHS Trust
Exemption 40 (2)	Devon STP
Exemption 40 (2)	Friary House Surgery
Exemption 40 (2)	Hospiscare
Exemption 40 (2)	Kinkerswell & Ipplepen Medical Practice
Exemption 40 (2)	Livewell Southwest
Matthew Spry / Joanne Fitzpatrick / **Malcolm Senior (SRO)**	NHS Devon CCG
Exemption 40 (2)	NHS Kernow CCG
Exemption 40 (2)	NHS Digital
Exemption 40 (2)	NHSX
Exemption 40 (2)	Northern Devon Healthcare NHS Trust
Exemption 40 (2)	Orion Health
Exemption 40 (2)	Plymouth City Council
Exemption 40 (2)	Royal Cornwall Hospitals NHS Trust
Exemption 40 (2)	Royal Devon And Exeter NHS Foundation Trust
Exemption 40 (2)	South West Ambulance Service Trust

	Exemption 40 (2) — St Thomas Medical Group Exemption 40 (2) — Torbay And South Devon NHS Foundation Trust Exemption 40 (2) — Torbay Council Exemption 40 (2) — University Hospitals Plymouth NHS Trust Exemption 40 (2) — HCRG (Devon Immunisations Team only) Exemption 40 (2) — Yeovil District Hospital
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	Kernow and Devon Local Medical Committees
Detail anything similar that has been undertaken before?	There are numerous shared/Integrated care record programmes that have been developed and are evolving throughout the UK. Examples of these using an Orion Health platform include: • Bristol, North Somerset and South Gloucestershire • Care and Health Information Exchange (covering Hampshire, Farnham and the Isle of Wight)

1. Categories, Legal Basis, Responsibility, Processing, Confidentiality, Purpose, Collection and Use

1.1.

What data/information will be used? Tick all that apply.	Tick or leave blank	**Complete**
Personal Data	✓	1.2
Special Categories of Personal Data	✓	1.2 AND 1.3
Personal Confidential Data	✓	1.2 AND 1.3 AND 1.6
Sensitive Data (UK GDPR Article 10 - usually criminal or law enforcement data)	✓	1.2 but speak to your IG advisor first
Pseudonymised Data	☐	1.2 and consider at what point the data is to be pseudonymised
Anonymised Data	☐	Consider at what point the data is to be anonymised
Commercially Confidential Information	☐	Consider if a DPIA is appropriate
Other	☐	Consider if a DPIA is appropriate

1.2.

Processing has to be lawful so identify which of the following you believe justifies what you are proposing to do and include an explanation as to why in the relevant box. You must select at least one from a – f.

Article 6 (1) of the GDPR includes the following:	
a) THE DATA SUBJECT HAS GIVEN CONSENT	**Tick or leave blank** ☐
Why are you relying on consent from the data subject? N/A	
What is the process for obtaining and recording consent from the Data Subject? (How, where, when, by whom). N/A	

Describe how your consent form is compliant with the Data Protection requirements? (There is a checklist that can be used to assess this). N/A	
b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY (The contract needs to be between the Controller and the individual and not concern data being processed due to someone else having a contract with the Controller. Processing can happen before the contract is entered into e.g. processing a pre-health assessment for a private or cosmetic procedure that is a paid for service with the delivery of that care done under contract between the Patient and the Practitioner).	**Tick or leave blank** ☐
What contract is being referred to? Click here to enter text.	
c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT (A legal obligation mandates processing of data as a task in itself where there are likely to be legal measures available if not adhered to e.g. an Employer has a legal obligation to disclose salary information to HMRC).	**Tick or leave blank** ☐
Identify the legislation or legal obligation you believe requires you to undertake this processing. Click here to enter text.	
d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON (This will apply only when you need to process data to protect someone's life. It must be necessary and does not only relate to the individual whose data is being processed. It can also apply to protect another person's life. Emergency Care is likely to fall into this category but planned care would not. You may need to process a Parent's data to protect the life of a child. The individual concerned is unlikely to be able to provide consent physically or legally; if you are able to gain consent then this legal basis will not apply).	**Tick or leave blank** ☐
How will you protect the vital interests of the data subject or another natural person by undertaking this activity?	
e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER (This is different to 6 c). If you are processing data using this basis for its lawfulness then you should be able to identify a specific task, function or power that is set out in law. The processing must be necessary, if not then this basis does not apply).	**Tick or leave blank** ✓
What statutory power or duty does the Controller derive their official authority from? Refer to the 'General Legal Gateway Matrix' – as set out in the Data Sharing Agreement	
f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY (Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. See the guidance for more information about the legitimate interest test).	**Tick or leave blank** ☐
What are the legitimate interests you have?	

Article 9 (2) conditions are as follows:	
a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT (Requirements for consent are the same as those detailed above in section 1.2, a)) N/A	**Tick or leave blank** ☐
b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐

c) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON WHERE THEY ARE PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT (Requirements for this are the same as those detailed above in section 1.2, d))	**Tick or leave blank** ☐
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	*N/A*
e) The data has been made public by the data subject	*N/A*
f) *For legal claims or courts operating in their judicial category*	☐
g) SUBSTANTIAL PUBLIC INTEREST (Schedule 1, part 2 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
h) PROCESSING IS NECESSARY FOR THE PURPOSES OF PREVENTIVE OR OCCUPATIONAL MEDICINE, FOR THE ASSESSMENT OF THE WORKING CAPACITY OF THE EMPLOYEE, MEDICAL DIAGNOSIS, THE PROVISION OF HEALTH OR SOCIAL CARE OR TREATMENT OR THE MANAGEMENT OF HEALTH OR SOCIAL CARE SYSTEMS AND SERVICES ON THE BASIS OF UNION OR MEMBER STATE LAW OR PURSUANT TO CONTRACT WITH A HEALTH PROFESSIONAL AND SUBJECT TO CONDITIONS AND SAFEGUARDS (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available). This is the primary lawful condition for the majority of access to DCCR to support delivery of safe and effective care.	**Tick or leave blank** ✓
i) PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, SUCH AS PROTECTING AGAINST SERIOUS CROSS-BORDER THREATS TO HEALTH OR ENSURING HIGH STANDARDS OF QUALITY AND SAFETY OF HEALTH CARE AND OF MEDICINAL PRODUCTS OR MEDICAL DEVICES, ON THE BASIS OF UNION OR MEMBER STATE LAW WHICH PROVIDES FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT, IN PARTICULAR PROFESSIONAL SECRECY (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH ARTICLE 89(1) BASED ON UNION OR MEMBER STATE LAW WHICH SHALL BE PROPORTIONATE TO THE AIM PURSUED, RESPECT THE ESSENCE OF THE RIGHT TO DATA PROTECTION AND PROVIDE FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT. (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available). N/A	**Tick or leave blank** ☐

1.3.

Confirm who the Controller and Processor is/are. Confirm if the Controller/s are solely or jointly responsible for any data processed?

(Identify any other parties who will be included in the agreements and who will have involvement/share responsibility for the data/information involved in this project/activity. Use this space to detail this but you may need to ask your DPO to assist you. Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only).

Name of Organisation	Role
Please refer to the membership of the Shared Care Record Programme Board – the organisations that are members of the Board will be Joint Controllers	Joint Controller
Any organisations that have access to ShCR data and contribute data to the ShCR, but that are not part of the ShCR Programme Board, will be Contributing Controllers	Contributing Controller
Any organisations that have access to ShCR data but do not contribute data to the ShCR, that are not part of the ShCR Programme Board, will be View only Controllers	View only controller
Amazon Web Services (AWS)	Sub-processor to Orion Health
Healthcare Gateway	Processor to Practices for MIG
Orion Health	Processor
NextGate	Solution partner providing patient matching tool used by Orion (NextGate do not have access to personal data)
Central programme support for Information Governance activities (subjects' rights, auditing - proactive/reactive, project DPIAs, IG leads engagement, reviewing informing materials, etc) provided by NHS SCW Commissioning Support Unit.	Processor

1.4.

Describe exactly what is being processed, why you want to process it and who will do any of the processing?

The DCCR brings together care data for service users from multiple sources into one single point of reference, where it can be accessed (subject to role-based permission & legitimate need to access) by care professionals, to help ensure they have the right information available at the right time to provide safe and effective care.

1.5.

Tick here if you owe a duty of confidentiality to any information. ✓

If so, specify what types of information. (e.g. clinical records, occupational health details, payroll information)

Yes, clinical and social care records.

1.6.

How are you satisfying the common law duty of confidentiality?

Reasonable expectations (please specify)

If you have selected an option which asks for further information please enter it here

Numerous studies/surveys/consultations have proven that the vast majority of the general public expect their data to be shared with or accessible to care professionals, when needed, to provide them with safe and effective care, and avoid them having to re-tell their story.
Aside from uses being within the 'reasonable expectations' of those to whom it pertains (in the vast majority of cases), the uses of data satisfy the common law duty of confidentiality on the basis of:

- Consent – there is implied consent through organisational approaches to informing individuals of the use of their data (a UK GDPR requirement under Articles 12-14), where individuals do not object to these uses. All end users will be encouraged to inform the individual, where possible of the access they are making. A communications strategy is also being established.

Should an individual object to information being shared through the ShCR – their ShCR may be made inaccessible (in its entirety) or the information may be restricted by controls in the contributing/feeder/source system (i.e. if a GP consultation or coded information is marked as confidential it will not flow through to the ShCR).

1.7.
Are you applying any anonymisation/pseudonymisation technique or encryption to any of the data to preserve the confidentiality of any information?
Yes

If you are then describe what you are doing.
Data is encrypted both in transit and at rest. It is also transmitted by whitelisted IP addresses/ports as an additional measure.

1.8.
Tick here if you are intending to use any information for a purpose that isn't considered as direct patient care. ☐

If so describe that purpose.
N/A

1.9.
Approximately how many people will be the subject of the processing?
Unknown - non-specific patient cohort
Approx. 1.7 million

1.10.
How are you collecting the data? (e.g. verbal, electronic, paper (if you need to add more selections then copy the last 'choose an item' and paste, the text has been left unlocked for you to do this.)
Other method not listed
Choose an item.
Choose an item.
Choose an item.
Choose an item.

If you have selected 'other method not listed' describe what that method is.
No new data is collected, but existing data from multiple sources is collated and presented as an overall view

1.11.
How will you edit the data?
N/A – data is a copy from Contributing Controllers' own electronic care record systems

1.12.
How will you quality check the data?

Testing routines to be determined to ensure data displays correctly – as data is a copy from Contributing Controllers' own electronic record systems it relies on existing data quality checks by those Controllers. Shared Care Records promote better data quality by virtue of the arrangement making it more likely data quality issues are detected (i.e. a staff member from another organisations accessing the record may report an inaccuracy). Any reported data quality issues will be passed to the source system controller for amendment that will then be reflected in the DCCR.

NextGate solution to be used by Orion Health, which has proven to significantly reduce duplication of records. DCCR to link to Personal Demographics Service to ensure up-to-date and reliable source of demographic data.

1.13.

Review your business continuity or contingency plans to include this activity. Have you identified any risks?

No

As the shared care record is a copy it will only provide additional resilience (i.e. it *may* not be accessible in the source system but available still in the shared care record system).
There are business continuity measures to ensure that the shared care record remains available (and the availability will become more imperative once there is greater reliance upon it, but ultimately if data is unavailable within the shared care record, then users can resort to existing means of access/sharing (via email, phone, etc).

If yes include in the risk section of this template.

1.14.

What training is planned to support this activity?

Training will be provided by Orion Health and resources available on Cornwall Partnership NHS FT's training site. There will be 'train the trainer' activities to help cascade across the system.
Organisations will be required to meet and maintain a 'qualifying standard' to join/access the DCCR, which includes meeting the Data Security and Protection Toolkit IG training compliance requirement, as set out in the Programme's Data Sharing Agreement.

2. Linkage, Data flows, Sharing and Data Opt Out, Sharing Agreements, Reports, NHS Digital

2.1.

Are you proposing to combine any data sets?

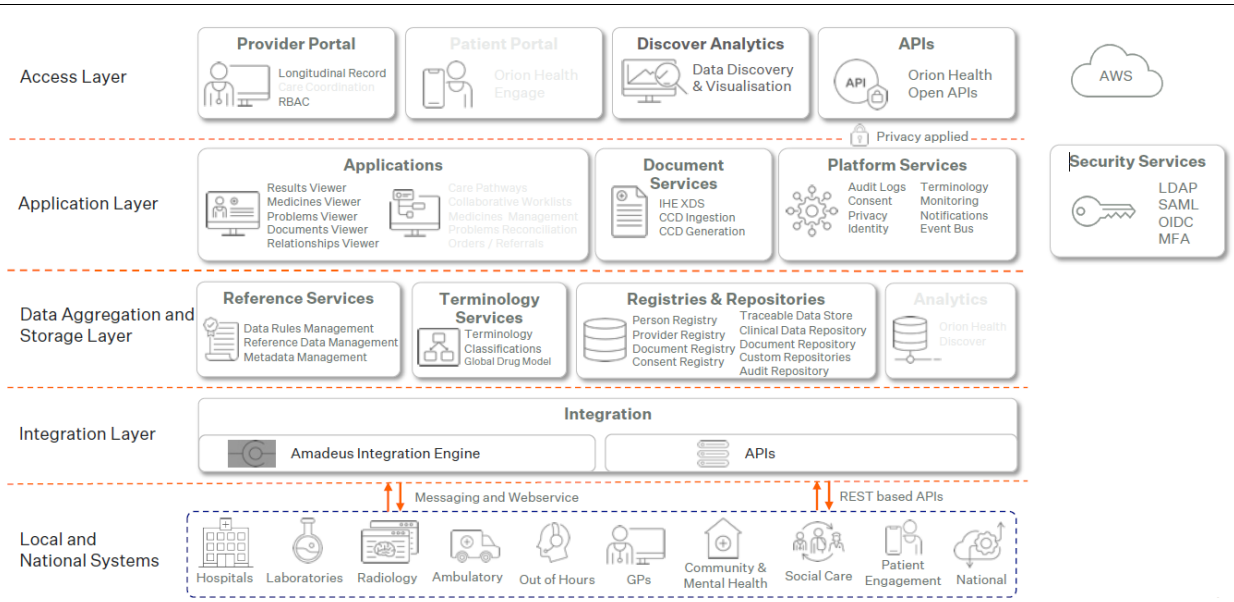
Yes

If yes then provide the details here.

The shared care record will bring together data on individuals that use health and social care services in Devon and Cornwall. The data that is combined will depend upon the data that each Contributing Controller agrees to share. This will constantly evolve. A central record of this will be maintained (as a 'living document').
Data will be linked to the national Personal Demographic Service ('PDS' also known as 'the spine') for which NHS Digital is the Controller to ensure the most up-to-date and reliable demographic information is used (noting any records flagged as 'sensitive' will have address details suppressed).
Data will be processed using a 'Medical Interoperability Gateway' which enables different datasets to be combined, but can also filter out certain coded data deemed to have additional sensitivity such as codes related to gender reassignment, sexual health & fertility).

2.2.

What are the Data Flows? (Detail and/or attach a diagram if you have one).



Note – 'Discover Analytics is for the production of reports on the usage of the shared care record, not analysis of the data within the record.

Contributing controllers will determine the data they flow from their source systems and how it maps to the DCCR and will be responsible for keeping accurate records of processing.

2.3.
What data/information are you planning to share?

Demographic information to enable the correct identification of individuals by those providing care and systems to match/look up data accurately (e.g. to enter a record via context launch or to combine data from the different sources.)

Data from individuals' health and social care records (dependent upon agreement/authorisation of Contributing Controller), is likely to include; medications, allergies, appointments, assessments, treatment, procedures, care plans, safeguarding concerns and risk alerts.

Again, this will evolve. A central record of what is shared will be maintained, linked to the programme's Data Sharing Agreement. Any substantive changes, where the risks are not already considered in this DPIA, will be considered in a new project DPIA.

This is to be led by clinicians and overseen by a Clinical Safety Officers (CSO) for Devon and for Cornwall.

2.4.
Is any of the data subject to the National Data Opt Out?

No - it is not subject to the national data opt out

If your organisation has to apply it describe the agreed approach to this

N/A

If another organisation has applied it add their details and identify what data it has been applied to

N/A

<u>If you do not know if it applies to any of the data involved then you need to speak to your Data Protection Officer to ensure this is assessed.</u>

2.5.
Who are you planning to share the data/information with?

Data is to be made accessible, subject to role-based controls/limitation/restriction, to members of health and social care services in Devon and Cornwall that can provide the required assurances (as determined by the Data Sharing Agreement) and are involved in the care of individuals.

2.6.
Why is this data/information being shared?
To support the provision of safe and effective care.

2.7.
How will you share it? (Consider and detail all means of sharing)
Data will be shared (either routinely in bulk data files or on a 'retrieve-on-demand clinical messaging' approach, dependent on source system capabilities) into a shared care record system from where it can then be accessed by health and social care professionals when necessary and subject to their role-based access.

Access will be by context launch where possible (access to individual's DCCR only by access to individual's record within their organisation's electronic patient record system). Some organisations may rely on access via a web-portal and username and password (subject to industry standard password complexity, refresh, limited attempts and delays, etc).

Tick if you are planning to use Microsoft Teams or another similar online networking/meeting solution that may have the facility to store or record conversations or related data as part of the sharing arrangements
☐

Provide details of how you have considered any privacy risks of using one of these solutions
N/A

2.8.
What data sharing agreements are or will be in place?
A data sharing agreement will be in place between all Contributing Controllers and Controllers not contributing but with 'view only' access. The DSA will define where controllers are considered to be joint and set out the responsibilities for all forms of controllers.

2.9.
What reports will be generated from this data/information?
There are no plans to generate reports (with the exception of usage performance reports and/or audit reports based on metadata) – the shared data is to be accessed when needed for the sole purpose of providing care to individuals. If in the future there is any proposal to use the data from the DCCR for other purposes, it will be subject to required impact assessment, consultation and agreement.

2.10.
Are you proposing to use Data that may have come from NHS Digital (e.g. SUS data, HES data etc.)?
Yes

If yes, are all the right agreements in place?
Yes

Give details of the agreement that you believe covers the use of the NHSD data
The programme will apply to interface with the personal demographics service for which NHSD is Controller.

If no or don't know then you need to speak to your Data Protection Officer to ensure they are put in place if needed.

3. Data Processor, IG Assurances, Storage, Access, Cloud, Security, Non-UK processing, DPA

3.1
Are you proposing to use a third party, a data processor or a commercial system supplier?
Yes

If yes use these spaces to add their details including their official name and address. If there is more than one then include all organisations. If you don't know then stop and try and find this information before proceeding.

Orion Health – for platform development, technical configuration, hosting (via AWS), issue support (may involve limited use of live data), testing purposes and staff training (limited to staff data) – Processing under contract with Devon Partnership NHS Trust, with Joint Controllers as 'third party beneficiaries to the contract.

Amazon Web Services (sub-processor of Orion Health) – host data centre

Devon Partnership NHS Trust – for user management (limited to staff data), website support and testing purposes (may not require any use of live data) – any processing as additional Joint Controller responsibilities

Central IG support – NHS SCW CSU – will be processing under agreement

3.2

Is each organisation involved registered with the Information Commissioner? Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Registered	Registration details or comments if not registered
Orion Health	Yes	Z8683942
NHS SCW CSU	Yes	Z2950066
	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.

3.3

What IG assurances have been provided to you and does any contract contain IG clauses that protect you as the Controller? (e.g. in terms and conditions, their contract, their tender submission). Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Brief description of assurances obtained
Orion Health & contracted sub-processors	**Assurances are in the contract with Devon Partnership NHS Trust** DSPT (see 3.4). Cyber Essentials Plus (Certificate number: IASME-CEP-002881). ISO 27001:2013 certified (approval number 00021380) with an information Security Management System (ISMS). The UK and Ireland business was certified as complaint by a UKAS-accredited external provider in December 2019. This work assures application of Orion Health's global Information Security Management System (ISMS) and associated controls to the UK and Ireland business. It also ensures that their security controls are continuously reviewed to maintain operational effectiveness in the UK and Ireland business. The scope of this approval is applicable to: Provision of interoperable Health Software Solutions from the UKI and third party hosting services. This includes sales, implementation and

	support functions being delivered to the public and private sector (in accordance with Statement of Applicability rev C). The NHS Digital guidance for connection to a Cloud service is also followed. The DCCR programme commissioned a cyber security assessment of the proposed data processing arrangements from DELT Shared Service Ltd (a copy of the report may be made available upon request). The executive summary notes *"All 14 Cloud security principles, as recommended by the NCSC [National Cyber Security Centre], have been identified as providing positive findings from the documentation reviewed".* This report will be circulated with the DPIA.
NHS SCW CSU	Centralised IG support. Limited personal data processing (data subject requests & auditing). DSPT (see 3.4). Cyber Essentials Plus (Certificate number: IASME-CEP-005575).
	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

3.4

What is the status of each organisation's Data Security Protection Toolkit?

DSP Toolkit

Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	ODS Code	Status	Published date
Orion Health	8HK91	20/21 Standards Exceeded (Orion Health confirmed that their DSPT has also been audited)	30/06/2021
NHS SCW CSU	0DF	20/21 Standards Exceeded (Audited)	29/07/2021
	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

3.5

How and where will the data/information be stored? (Consider your answer to 2.7 and the potential storage of data in any online meeting or networking solution).

Cloud hosted by Orion Health using AWS

3.6

How is the data/information accessed and how will this be controlled?

Front end users will access through either 'context launch' (access to individual's DCCR only by access to individual's record within their organisation's electronic patient record system) as a default or where 'context launch' is not technically feasible via a web-portal by username and password (to industry standard requirements for complexity & refresh).

Access to data will be based on Role Based Access Controls, following the NHSX RBAC model. Partner organisations will as part of onboarding of their data have control which data items go into which categories in the RBAC model. For General Practices, the MIG sets out the data extracted and presented for practices - it is

the detailed care record spec here - **https://healthcaregateway.co.uk/solutions/detailed-care-record/**. Partner organisations will also determine the relevant RBAC role for their staff accessing the system:

Devon and Cornwall Care Record RBAC Ma

The RBAC will be maintained and overseen by the Programme's Clinical Cabinet. It is common to see variation in use of roles, often reflecting different ways of working from one organisation to another. Each organisation will be responsible for the correct allocation of a role to their users. The RBAC matrix has examples of the sorts of job roles an RBAC role relates to. Organisations won't routinely know what other organisations have given their staff access to, but the allocation is an organisational responsibility, therefore any possible incident as a result of the wrong role (too much or too little) is ostensibly an individual organisational problem. Experience of other such programmes is that variance does come to light in general use and development discussions, and often leads to some review of the RBAC set up, possibly creation of new roles.

N.B. For 'context launch', users establish a 'legitimate relationship' with the individual (whose record is to be accessed) when accessing the individual's record in their own organisation's electronic patient record. In respect of portal access, the programme decided it would not implement a 'challenge screen' to record staff members' legitimate relationship. This decision was informed by the benefits and disbenefits established by other programmes (who have, on the whole, either proceeded without a 'challenge screen' or recently removed it). The programme has also decided that it will not implement 'break seal' functionality, the consensus view was that data should either be shared via the DCCR or not shared.

3.7

Is there any use of Cloud technology?

Yes

If yes add the details here.

Orion health will host data using AWS as a sub-processor.

3.8

What security measures will be in place to protect the data/information?

Orion Health applications are penetration tested on an annual basis for AWS customers (as per the terms of the contract). The Pen Test company have CREST, CHECK, UKAS and ISO 17025 accreditations/certifications. (An attestation letter or high level summary of the test can be provided on request).

Orion Health run a monthly security scan as part of the monthly patching schedule for hosted customers. The Report is sent to Orion Health's Security Team to review and comment on any vulnerabilities present at that time.

Data is encrypted in transit and at rest with 256 AES encryption; for HL7 Orion Health use TLS1.2 encryption and SFTP for flat files which uses shared key authentication and is encrypted using the SSH protocol (which SFTP is based on). The keys are at least 2048bits and AES256. Whitelisting is also used (as an additional measure, not on its own).

Orion Health apply patches on a monthly basis for hosted customers in accordance with their 'Patch and Vulnerability Management Policy' (available on request).

Independent penetration testing to be commissioned by programme.

Is a specific System Level Security Policy needed?

Yes

3.9

Is any data transferring outside of the UK? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)
Yes

If yes describe where and what additional measures are or will be in place to protect the data.
Whilst there will be no routine transfers of data outside of the UK, it is likely that Orion Health will, at some point, access/use data for the purpose(s) of support and/or testing. This is likely to be from within New Zealand, for which there is an 'adequacy decision'.

Should there be a need in the future for Orion Health to access/use data from a territory without an 'adequacy decision', the affected Controllers would first need to ensure that they have completed a Transfer Impact Assessment and put in place Standard Contractual Clauses.

It is also noted for completeness of risk assessment that Orion work with a Managed Security Service Provider (MSSP) that is based in the USA and that logs related to the system are sent to the MSSP for evaluation of any potential security events.

These logs do not contain any personal data. They are infrastructure, operating system security event and host based security tooling logs (covering anti-malware, File Integrity Monitoring, Intrusion Detection System/Intrusion Protection System). On that basis this is not a transfer of personal data outside of the UK.

3.10
What Data Processing Agreement is already in place or if none, what agreement will be in place with the organisation and who will be responsible for managing it?
Contract in place with Orion Health between them and Devon Partnership NHS Foundation Trust, which links all other parties as primary agencies as part of the contract.

4. Privacy Notice, Individual Rights, Records Management, Direct Marketing

4.1
Describe any changes you plan or need to make to your Privacy Notice and your proposed completion date? (There is a checklist that can be used to assess the potential changes required or if you wish for it to be reviewed then add the link below).
Each partner contributing to and/or viewing the DCCR will be required to ensure that their organisational Privacy Notice includes sharing via the DCCR. A central website will be created to support organisational privacy notices so that further detail is available and consistent across all partners. Other materials to support may also be developed and provided to all partners.

Staff using the system will be encouraged to inform individuals, where possible and appropriate, about accessing the DCCR when they are providing care to them. Communications will be issued to staff/end users to help ensure a consistent approach is taken. Whilst it constitutes a reasonable step to comply with UK GDPR Article 12-14, it also supports partners' duty of candour to patients (regarding transparency).

4.2
How will this activity impact on individual rights under the GDPR? (Consider the right of access, erasure, portability, restriction, profiling, automated decision making).
To be informed – organisations must inform individuals of the purposes for processing their personal data, the retention periods for that personal data and who it will be shared with. Organisations should already provide this information to individuals. UK data protection laws do not require organisations to detail the means by which they are sharing information, however, Joint Controllers are required to be transparent about their respective responsibilities which would be difficult without the detail of the programme. Also, in the interests of transparency it is deemed best practice that reasonable steps are taken to make individuals aware of processing involved in such programmes. (see 4.1 above)

Access – the Joint Controller responsibilities within the DCCR will have implications for individuals that exercise their right of access, for example, if a subject requests a copy of all their data from a Joint Controller this would potentially include data contributed to the DCCR by a number of other Controllers. The handling of such requests will be set out in programme policy and procedure.

Objection – the Programme has agreed that objections to sharing between organisations will be handled as they would prior to the DCCR, however given there is no limitations to the right to object, and so an objection may be specific to sharing through the DCCR, it is agreed, to ensure consistency, such an objection will be upheld after establishing that the individual has capacity, is fully informed of the risks and understands the potential implications. The functionality currently offered by the Orion Health solution to handle upheld objections is limited to making all shared data inaccessible to users.

Additionally if a patient's record on the national PDS system is flagged as 'sensitive' (s-flagged) then data on their address will be suppressed.

Restriction – generally only applies whilst right to object or rectification are being considered and where the subject has requested restriction. Any controller receiving a request to restrict whilst dealing with a rectification or objection will consider using functionality to prevent sharing of the record whilst the rectification or objection request is concluded, noting possible clinical/care risks from restricting the sharing at least temporarily.

Rectification – As the DCCR is only intended to enable sharing of a copy of data, any rectification would need to be handled by the affected Controller as they would prior to the DCCR.

Erasure – very unlikely to apply to data processed via the DCCR, as generally only applies where data is processed on a basis of consent or legitimate interests (UK GDPR Article 6,1a or 6,1f - neither of which apply to data processed via the DCCR)

Portability – very unlikely to apply to data processed via the DCCR, as generally only applies where data is processed on a basis of consent or for the performance of a contract (UK GDPR Article 6,1a or 6,1b).

Automated decision making – will not apply to data processed via the DCCR as no automated end-to-end decision making is planned as part of the DCCR.

4.3

How long is the data/information to be retained?

Where data is retrieved on demand, data going back at least two years will be displayed but will not be retained. For data that persists it will be retained in the DCCR environment for the same period as the source system and purged at the point that the Contributing Controller excludes the data from their data feed (i.e. data is removed from the Controller's own record system).

4.4

How will the data/information be archived?

Data in the DCCR will not be archived other than detail of user activity in the audit trail, which will be persisted for lifetime of the system, may be archived offline for very long running solutions.

4.5

What is the process for the destruction of records?

Records that are deleted in line with deletion from source systems are triggered by the updated data files that note the change. The contract with Orion details how records will be handled at the point of termination of the contract. That will either be a transfer to a new supplier or provision of the records to the partner organisations if the system is to be decommissioned.

As the data is electronic any passing of the records to a new supplier or back to the NHS does itself not delete the records from the infrastructure. Once transfer has been confirmed as complete, then any remaining copy on the storage infrastructure will be logically deleted.

4.6

What will happen to the data/information if any part of your activity ends?

See 4.5

4.7

Will you use any data for direct marketing purposes? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

If yes please detail.

N/A

5. Risks and Issues

5.1

What risks and issues have you identified? The DPO can provide advice to help complete this section and consider any measures to mitigate potential risks. The table in this section identifies the risks and scores prior to any mitigation controls being identified and assessed.

Risk	Likelihood of harm 1- Very Low 2- Low 3- Medium 4- High 5- Very High	Severity of harm 1- None 2- Low 3- Medium 4- High 5- Very High	Overall risk
Unauthorised/ inappropriate access - external hacking threat	3	4	12
Unauthorised/ inappropriate access - end user inappropriate access	3	4	12
Poorly managed user access could result in account sharing (devaluing audit data) or an increased risk of unauthorised/inappropriate access	2	4	8
Over-sharing of personal data	2	3	6
Loss / unavailability – accidental loss or theft	2	4	8
Data is of poor quality	3	3	9
Unlawful processing - processing personal data without a lawful basis	2	4	8
Failure to adequately inform individuals about the use of their personal data	3	2	6
Data retained for longer than necessary	3	2	6
Failure to complete DPIA, where required, prior to new processing	2	3	6
Failure to maintain a record of all categories of processing activities - there is a legal requirement on Controllers and Processors to maintain a record of all categories of processing activities	2	3	6
Failure to manage/ report incidents - there is a legal requirement to report incidents (that have or are likely to result in a risk to the rights and freedoms of individuals) to the supervisory authority (ICO) within 72 hours of becoming aware.	2	3	6

Failure to manage subject rights in an appropriate manner - there is a legal requirement to respond to requests from individuals to exercise their rights in respect of their personal data.	3	3	9
System failure – i.e. opt out functionality fails to prevent access	1	3	3
Data is used for purposes outside of the Data Sharing Agreement	2	4	8
Audit history in patient apps/GP record access does not necessarily report useful clear audit trail data back to the patient	5	2	10

5.2

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in 5.1				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Unauthorised/ inappropriate access - external hacking threat	Complex password requirement with limited attempts or context launch (so subject to Controllers' systems password security requirement). Encrypted transmissions of data. System security perimeters (local firewalls and physical access controls). Routine penetration testing by Orion Health and programme to expose vulnerabilities and improve system security. Orion Health applies security patches on monthly basis. User accesses pane (highlighting potential inappropriate access to users). Acceptable use message(s)/policy. Caching of documents from web portal prevented.	Reduced	Medium	
Unauthorised/ inappropriate access - end user inappropriate access	All users subject to Controllers' compliance requirements including annual Data Security training. User accesses pane (highlighting potential inappropriate access to users). Acceptable use message(s)/policy. Caching of documents from web portal prevented. Context Launch limiting access to patients registered in users	Reduced	Medium	

	organisational system, preventing browsing all records in the ShCR			
Poorly managed user access could result in account sharing (devaluing audit data) or an increased risk of unauthorised/inappropriate access	Phased implementation/roll-out with checks on user access management process. Some/most access linked to source system access. All users subject to Controllers' compliance requirements including annual Data Security training. Acceptable use message(s)/policy. Controller starter/change/leaver processes. Controllers' compliance activities to monitor/identify such behaviour. System training and user guides.	Reduced	Low	
Over-sharing of personal data	Phased implementation/roll-out of sharing with authorisation from Controllers of affected data. Policy/procedure ensuring new data sharing is assessed. All Controllers' staff with access to DCCR should be bound to maintain confidentiality under contract (and most under professional code of conduct too). Controllers' compliance requirements including annual Data Security training.	Reduced	Low	
Loss / unavailability – accidental loss or theft	System security, resilience and back up routines. Services' business continuity plans (i.e. revert to former methods of accessing / sharing data such as emailing). User communications.	Reduced	Low	
Data is of poor quality	Controller commitment through Data Sharing Agreement. Change control processes. Routine system checks. System training and user guides. Use of Nextgate solution and PDS to cross-match data.	Reduced	Low	
Unlawful processing - processing personal data without a lawful basis	Establishing appropriate governance arrangements; review by information	Reduced	Low	

	governance subject matter experts.			
Failure to adequately inform individuals about the use of their personal data	Controller commitment through Data Sharing Agreement. Inclusion of assurance on the approach, method and materials included in on-boarding process.	Reduced	Low	
Data retained for longer than necessary	Establishing appropriate governance arrangements; review by information governance subject matter experts and by health and social care professional's determining the need to retain.	Reduced	Low	
Failure to complete DPIA, where required, prior to new processing	Establishing appropriate governance arrangements; review by information governance subject matter experts.	Reduced	Low	
Failure to maintain a record of all categories of processing activities - there is a legal requirement on Controllers and Processors to maintain a record of all categories of processing activities	Establishing appropriate governance arrangements; review by information governance subject matter experts.	Reduced	Low	
Failure to manage/ report incidents - there is a legal requirement to report incidents (that have or are likely to result in a risk to the rights and freedoms of individuals) to the supervisory authority (ICO) within 72 hours of becoming aware.	Controller commitment through Data Sharing Agreement. Controllers' compliance requirements including annual Data Security training.	Reduced	Low	
Failure to manage subject rights in an appropriate manner - there is a legal requirement to respond to requests from individuals to exercise their rights in respect of their personal data.	Controller commitment through Data Sharing Agreement and issue of standard operating procedure. Controllers' compliance requirements including annual Data Security training.	Reduced	Low	
System failure – i.e. opt out functionality fails to prevent access	The Orion Health platform has tried and tested 'opt out' functionality Change control processes. Routine system checks. Programme policy/procedure.	Reduced	Low	

Data is used for purposes outside of the Data Sharing Agreement	Acceptable use message(s)/policy. System training and user guides.	Reduced	Low	
Audit history in patient apps/GP record access does not necessarily report useful clear audit trail data back to the patient	Transparency materials. Development of prepared statement to respond to such concerns arising. Known issue raised nationally with NHSE and NHSX.	Reduced	Low	

5.3
What if anything would affect this piece of work?
Not known

5.4
Please include any additional comments that do not fit elsewhere in the DPIA?
N/A

6. Consultation

6.1
Have you consulted with any external organisation about this DPIA?
No

If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.
No consultation has taken place outside of the group of partner organisations. This is because the general concept of shared care records is not new to the health and care sector and nearly all Integrated Care Systems already have a form of shared care record. Should any partner propose the need to consult with any external organisation that will be considered.
There are however plans to consult with General Practices and Local Medical Committees.

6.2
Will you need to discuss the DPIA or the processing with the Information Commissioners Office? (You may need the help of your DPO with this)/
Don't know

If yes, explain why you have come to this conclusion.
Whilst the above answer is 'don't know' that is on the basis the risks assessed above need to be consulted on with all partner agencies. Currently the mitigated risks are below the threshold for ICO consultation, however should partner consultation come to a different conclusion and any risk subject to mitigation be re-assessed as high, then ICO consultation will be necessary. Following partner consultation this section of the DPIA will be amended accordingly.

7. Data Protection Officer Comments and Observations

7.1 Comments/observations/specific issues	These will be gathered from partner organisation DPOs during a period of consultation

8. Review and Outcome

Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:
A) There are no further actions needed and we can proceed

If you have selected item B), C) or D) then please add comments as to why you made that selection

We believe there are
A) No unmitigated or identified risks outstanding

If you have selected item B) or C) then list these in the amber boxes below and then consider additional measures you could take and include these in the green boxes below

Residual risks and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above (B and C)				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved (SIRO)**
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Signed and approved on behalf of Click here to enter text.

Name: Click here to enter text.

Job Title: Click here to enter text.

Signature: Click here to enter text. Date: Click here to enter a date.

Signed and approved on behalf of Click here to enter text.

Name: Click here to enter text.

Job Title: Click here to enter text.

Signature: Click here to enter text. Date: Click here to enter a date.

Please note:

You should ensure that your Information Asset Register and Data Flow Mapping Schedules are updated where this is relevant.

This DPIA can be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure detail them here:
Click here to enter text.