Dorset HealthCare University NHS Foundation Trust

Data Protection Impact Assessment Form

Dorset Intelligence and Insight Service (DiiS) V2.8

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 Dorset Intelligence & Insight Service (DiiS) is a collaborative Service delivering a near real time, live, linked health and social care dataset across the Dorset Integrated Care System (ICS). The aim is to make health and social care data open, easy to access, and available to create actionable insights. It is being used to support data-led service improvement, planning and decision making at a System and organisational level – and at a local level during Dorset's COVID-19 response. We've been working together from the start with partners, community groups, and industry to provide analytics to deliver better health and wellbeing outcomes for Dorset people. The DiiS is being used every day by health and care professionals across Dorset to make evidence-based decisions to improve the health and wellbeing of our population. This was particularly evidenced during the COVID-19 pandemic, where the DiiS became a tool at the forefront of Dorset's analytical response linking data from primary care, acute, ambulatory and community providers on a near real time basis. Other examples of this include: • Case finding/Targeting for individuals or cohorts (including secure re-identification of patients or service users to those who manage their care) • Population Health Management (PHM): the ability to group by medical, mental health, demographic and socio-economic markers to identify points of earlier intervention in the pathway • Provision of wider population-based insights to enable the use of social prescribing Further detail on the programme, and the Service that it has delivered is available in the DiiS Strategic Outline Business Case (SOBC).

This is one of the first data repository systems to be developed under the Dorset ICS Partnership (Integrated Care System), serving all the ICS Partner organisations. In its role as a provider organisation Dorset HealthCare (DHC) has agreed to host the architecture on behalf of the ICS meaning that it will hold PID information from other organisations that has been pseudonymised at source (as per the later diagram). The benefits of linking health and social care data for use within PHM, producing service efficiencies and improving the experiences of the patient are clear. As DHC is able to do, and it has an interest across the county, it was a logical step that the DiiS warehouse be hosted by DHC, within a Microsoft Azure capability developed in house.

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?
To run the DiiS, data will be obtained through various systems, including internal established ICS partner data warehouses as these become available or their current equivalent through APIs, or CSVs from individual data bases for example. The standard approach to securely extracting and loading data from external systems and into the DiiS is displayed below. Any variations to this for specific systems or organisations will be documented and added into the technical documentation set and then available upon request. Data is downloaded in comma separated value (CSV) format to a secure network folder within the DHC domain. The individual files are then combined into one zip file and transferred to an FTPS (File Transfer Protocol Secure) server. Data is then transferred from the FTPS server into the staging environment where it is extracted, cleansed, and correlated, before being loaded through to the central data warehouse, data mart, and Analysis Services database. Various Power BI reports displaying the correlated data held within the Analysis Services database will be produced and providing insights and focus on various clinical, population and service areas.

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 data to be processed is: • Primary care data from all GP Practices across Dorset • Mental health data set (MHSDS) – provided by DHC • Steps to Wellbeing / IAPTUS – provided by DHC • CSDS –provided by DHC

- Acute Hospital data from local Acute Trusts (including UHD, DCH, Yeovil & Salisbury and /or alternatively SUS feeds) for COVID
- SUS Acute data feed from NHSD / DSCRO
- ECDS from NHSD / DSCRO
- SWAST 111 and 999 telephony data from DHC
- Drugs and Alcohol data from Public Health Dorset
- Patient level data from the Somerset Cancer Registry (SCR)
- Safeguarding flags from GP instances of SystmOne
- Data from out of area Acute Trusts will be only collated for Dorset GP registered patients, at the time of writing this is for COVID test results and the Somerset Cancer Registry dataset.
- COVID test result data from all Dorset related sources, including Yeovil and Salisbury Foundation Trusts.
- Workforce data - from DHC, DCH and UHD (and planned to also be received from the ICB)
- CY&P Social Care dataset – from Dorset and BCP Councils

Data will be received and processed daily, from some services and others on a regular basis. "Regular" will be defined as per each dataset, and will be available from within the DiiS, saving the frequent updating of this document. Wider details on the frequency and methodology of these feeds are available from within the DiiS team.

Data held within the secure network folder will be held solely to provide patient level data to the DiiS reporting solution, which will include tried and tested analytical capabilities from third party suppliers but will remain within the DiiS infrastructure. For example, any purchased risk stratification tool will be placed within the DiiS architecture meaning that data will be managed and held within the approved locations of DHC.

Access to DiiS will be managed through role based access controls (RBAC), the detail and processes which support this are available under separate cover. The RBAC documentation is available on request. Where specialist external services / contractors are used, they will be requested to sign an additional non-disclosure agreement (NDA) to reflect a consistent approach of managing data protection in the same way as standard NHS employment contracts. These will be monitored by DHC's DPO lead and the DiiS Management Team.

The DiiS will also be providing analytics and intelligence for the Wessex Cancer Alliance (WCA) which geographically covers Dorset and Hampshire. The data collected as part of this service is covered under a separate Joint Controller & Data Sharing Agreement between DHC as processor of the data and the HIoW Trusts who will be sharing the information. This can be made available upon request and is simply not linked within this document for reasons of version control.

The data will be reviewed on a maximum of six-yearly basis (physical health) and a maximum of twenty years (mental health). At present all data is being used within the Service, and now that we have moved into the PowerBI app, we can understand the numbers of reports that are used within what timescales.

As detailed within the RBAC documentation, reviews will be undertaken on a quarterly basis on which reports and which accounts have been accessed. For those accounts that have not been used, users will be sent an email enquiring whether the account is still required or whether it should be terminated. If no response is received the account will be terminated. Upon termination the user will need to reapply from scratch. If a report has not been accessed within three months, it will be escalated to the DiiS Senior Management Team (SMT) for review as to whether the report should be suspended or decommissioned.

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)?

The individuals whose data is being processed are patients or service users of the ICS and does include children and vulnerable adults.

Primary care providers have been asked whether they wish to participate going forwards however patient consent is not required for data to be shared with the DiiS. The anonymity of all patients will be ensured at all times by stripping PID data from supplied files. Once the data is removed, no one using the data will be able to identify patients within the DiiS reports and dashboards so patient consent is not required. DiiS has the ability to recognise opt out codes so for patients who have opted out of sharing their data, it is not taken from the Practice and therefore is not received into DiiS. DiiS takes daily delta updates from SystmOne meaning that any changes to patient opt outs will be picked up every 24 hours.

It has been agreed within the Dorset IG community that DiiS can operate without implementation of opt outs, as the data entering the DiiS is pseudonymised and contains no exact DoB and/or exact Postcode. This decision has been made due to following the National Data Opt-Out Operational Policy Guidance, which states 'If the information has been anonymised in line with the Information Commissioner's Office's Anonymisation Code of Practice, the national data opt-out

does not apply. You can share anonymised data, and people do not have the power to opt out of this.'"

The extraction methods from the contributing systems are tried and tested, and therefore offers no additional risk. Data will be held on DHC sites and therefore will be subject to existing protections. The DiiS Development team will work with providers of data to deploy and test the pseudonymisation tool that we have created to offer additional data protection. This will ensure that the pseudonymisation tool is securely established within a providers' network and can send through uniquely pseudonymised data into the DiiS.

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 development of the Dorset Intelligent and Insight Service (DiiS) is to enable the embedding of a culture of data and intelligence sharing, including population health management across the Dorset ICS in order to improve patient and population health, care and well being outcomes. This will be done through the analysis of linked datasets including data provided from all partners within Dorset. This linked data will be interpreted through reports designed by analysts and clinicians working collaboratively to understand the data and ensure its integrity and quality.

The reports will then be used to inform decision making on the treatment of cohorts of patients, the services needed to support those patients, the highlighting of inequalities and numerous other uses. The reports and dashboards that are the front-end outputs will present pseudonymised record level and aggregated data.

The outcomes from the DiiS continue to feed into the development of a population health management capability for Dorset. This capability enables segmentation and risk stratification for diseases and inequalities alongside further research across health and care services to improve the service for our population.

A re-identification capability is available through the DiiS, allowing clinicians to re-identify the NHS number of patients of whom they have the care. This capability to best described through an example, where a GP has identified a number of patients who have regularly have breathing difficulties that may lead to more serious issues in the future, they can request that that cohort of unique

pseudonymised IDs be re-identified back to their NHS number. The GP can then check those NHS numbers against their own primary care system to find the PID relating to those NHS numbers. A limited number developers and analysts within the DiiS team are able to reidentify patients, for reasons of testing this reID process and supporting clinicians. Nor will other clinicians have access to NHS numbers that don't belong to their patients. Demonstrations of this capability with test data are available through the DiiS Team. This will allow clinicians to work with patients with symptoms or early onset conditions that they may previously have been unaware of and prevent or delay those conditions, and patients, deteriorating.

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?

The use of the TPP strategic reporting tool as the source for primary care data was agreed with DHC's Clinical Systems Manager, DHC's Clinical Lead for SystmOne, and DHC's Lead Systems Specialist. The reports that are produced using the data from this extraction will be developed between DiiS analysts and lead clinicians in the relevant areas within primary or acute care or service providers within Local Authorities and Public Health.

The architecture for the solution has been agreed in consultation with Microsoft infrastructure experts as well as the DHC infrastructure team. Additional consultancy support will be obtained through trusted NHS partners in order to confirm and test the architectural design and resiliency.

Once the architecture is sufficiently established, the DiiS team will request security review and testing of the system by trusted NHS partners, including but not limited to Penetration testing of the DiiS. The plans and outcomes from this will be shared with the DiiS Board, DHC IG Steering Group and Pan Dorset IG Group as required. The penetration test and business continuity reviews are planned for Q1 2023. The DiiS team has worked alongside the WCR Cyber assurance team to ensure clear communication and compliance with the aims of the WCR programme.

The DiiS team have presented the DiiS system, its use and the current patient outcomes to the Our Dorset Public Engagement Group (PEG) in Q3 2019, December 2021 and to the Digital PEG in July 2022. This was expected to be an annual consultation and engagement approach but for the disruptions presented by the coronavirus pandemic. DiiS expects to have a member of the Our Dorset Digital Public Engagement Group (DPEG) join its Board in Q1 2023.

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?
In order to enable the ICS to operate a population health management approach, the linking of data from multiple health and care systems is essential. The DiiS will enable the removal of some siloed working across the ICS and build the ability to plan services and treat patients regardless of the data holding their information. The datasets will be provided from source, within the contributing organisations, and therefore work will be undertaken with those organisations to identify and correct any data quality issues. The DiiS, and the data quality requirements, are part of the Dorset Trust quality assurance group, meaning that issues can be addressed and resolved with all the relevant partners and plans for wider future consistency can be agreed. The DiiS team will continue to work with the DiiS Board, Clinical Reference Group (CRG), Finance Reporting Group (FRG) and the Pan Dorset IG Group enabling a level of assurance to be provided across all user functions within the ICS Partnership. Data will be held within an Azure tenancy within Dorset HealthCare network and so will be managed in conjunction with the existing security frameworks and processes of the Trust. As the DiiS will be hosted within a DHC environment it is not anticipated that the data will be subject to international transfers. The following is the legal basis for processing patient information within the DiiS, from GDPR: We only process your information if we have a lawful reason to do so. We make sure you know how we use your information, and tell you about your rights. This

will be done through the Privacy Notices available on GP, Trust, Local Authority and other relevant websites.

We rely on the following specific conditions in Articles 6 and 9 of the GDPR to process patient information:

6(1) (e) '…for 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…'

Step 5: Identify and assess risks

10

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**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
1. Exposure of individuals medical records	Remote	Severe	Medium
2. Risk of system breach by means of adverse cyber security	Remote	Severe	Medium
3. There is a risk that function creep may occur	Possible	Significant	Medium
4. There is a risk that records will not be removed / will continue to flow once the COPI guidelines have ceased	Remote	Severe	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**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
1. Exposure of individuals medical records	All data is pseudonymised at source meaning that patient records in the clear are not viewable within the DiiS. Should this occur then the team would work with the DPO to follow the correct procedures to resolve the issues	Reduced	Low	Yes
2. Risk of system breach by means of adverse cyber security	The DiiS architecture sits within the DHC network and therefore sits within their protections. Continue to work with the DHC ICT team to ensure these remain valid. Continue to work with the WCR Cyber team to ensure best practice.	Accepted	Low	Yes
3. There is a risk that function creep may occur	New projects / work streams are raised at the DiiS Board, Clinical and IG leads, to ensure these are useful and fit with the plans of the Service.	Reduced	Low	Yes
4. There is a risk that records will continue to flow once the COPI guidelines have ceased	The Team will continue to engage with NSHE/I regional teams as well as the local DPOs to ensure we remain informed as to when the COPI guidance changes. This process has worked to date as we are advised in a timely	Reduced	Low	Yes

	manner when the guidance has been extended.			

Step 7: Sign off and record outcomes

DPIA Reviewed & Updated:	Heather Case 17.01.2023	This version updated to remove Confidential information such as architecture diagrams.
	Paddy Baker ICB DPO	
DPIA Reviewed & Updated:	Heather Case 30.12.2022	Document updated with general amendments to reflect the changes made to the Service especially in terms of new datasets added and the move from a CCG to an ICB and ICS.
Measures approved by:		*Awaiting review at Pan Dorset IG on 20.01.2023*
This DPIA will kept under review by:	Heather Case – Head of DiiS Pan Dorset IG Group	The DPO should also review ongoing compliance with DPIA
DPIA Reviewed & Updated:	Heather Case 17.01.2022 Head of DiiS Matt Prowse 17.01.2022 Head of BI	Updates made following review by NHSD and includes all recommended comments on the DPIA.
Measures approved by:	Dave Way DHC DPO 19/01/2022	

DPIA Reviewed & Updated:	Heather Case 25.06.2021 Head of DiiS	Various updates made on DiiS architecture, datasets and purpose for collecting the data. Reviews and amendments also made through consultation and

		review by DPOs from DCCG and DCH.
From 2022, it is anticipated that this document will be reviewed by the Pan Dorset IG Group as there are representatives from all the ICS partners at that Group meaning that we were be able to ensure consistency and clear communications across the ICS partners.		

Item	**Name/date**	**Notes**
Measures approved by:	Dave Way DHC DPO 24/06/20	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	N/A	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Dave Way DHC DPO 24/06/20	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: 1. Following the successful PoC phase the DiiS team must ensure any additional requirements, contractual arrangements or changes to processes are shared with the DPO and acceptance of changes logged. 2. Where information is anonymised and pseudonymised checks should take place to ensure that is the case and any breaches reported immediately to the DPO. 3. The DiiS must inform the DPO of any structural IT changes such as any changes to server locations or technical changes to flows in data transfers		
DPO advice accepted or overruled by:	Heather Case 24/06/20	If overruled, you must explain your reasons
Comments: DPO Comments accepted.		
Consultation responses reviewed by:	Heather Case and Chris Jenkins 12.12.2018	If your decision departs from individuals' views, you must explain your reasons

Comments:

All persons consulted are content with the approach and planned outcomes.

12.02.2020: DPIA updated as part of a regular review of IG documentation

10.03.2020: DPIA Updated to reflect the closure of the Proof of Concept phase and the move from the Intelligent Working Programme to a business as usual Dorset Intelligence and Insight Service (DiiS).

24.06.2020: DPIA updated to include the COVID related feeds from Salisbury and Yeovil and planned data feeds from Cornwall GP Practices and wider STP partners.

25.06.2021: Please note that as a result of the COVID pandemic and the more advanced state of the Kernow CCG and STP, data sharing with Kernow did not take place. Rather a relationship of consultancy will continue between Dorset and Kernow.

12.2021: Updated following the introduction of Role Based Access Controls (RBAC) and the Microsoft PowerBI app.